D-Link®

Version 1.01 | 06/06/2014

User Manual

Wireless AC Dual-Band ADSL2+ Modem Router

GO-DSL-AC750

Preface

D-Link reserves the right to revise this publication and to make changes in the content hereof without obligation to notify any person or organization of such revisions or changes.

Manual Revisions

Revision	Date	Description
1.0	February 24, 2014	• Initial release for Revision A1
1.01	June 06, 2014	• change Model description

Trademarks

D-Link and the D-Link logo are trademarks or registered trademarks of D-Link Corporation or its subsidiaries in the United States or other countries. All other company or product names mentioned herein are trademarks or registered trademarks of their respective companies.

Copyright © 2014 by D-Link Systems, Inc.

All rights reserved. This publication may not be reproduced, in whole or in part, without prior expressed written permission from D-Link Systems, Inc.

Table of Contents

Preface i
Manual Revisions i
Trademarks i

Product Overview 1
Package Contents 1
System Requirements 2
Introduction 3
Features 4
LEDs 5
Back 6
Hardware Overview 7
Left 7

Installation 8
Before you Begin 8

Wireless Basics 9
Wireless Installation Considerations 10
Installation 11
Connect a Wireless Client to your Router 12
WPS Button 12

Configuration 13
Web-based Configuration Utility 13
Setup Wizard 14

Manual Configuration 20
Setup 20
Internet Setup 21
2.4G Wireless 23
2.4G Wireless Security 24
5G Wireless 25
5G Wireless Security 26
Local Network 27
Local IPv6 Network 29
Time and Date 30
Advanced 31
2.4G Advanced Wireless 31
Advanced Settings 32
MAC Filtering 34
Security Settings 35
WPS Settings 36
5G Advanced Wireless 37
Advanced Settings 38
MAC Filtering 40
Security Settings 41
WPS Settings 42
ALG 43
Port Forwarding 44
Port Trigger 45
DMZ 46
SAMBA 47
3G WAN Configuration 48
Parental Control 49
Website Filter 50

MAC Filter 51
Filtering Options 52
IPv4 Filtering 53
IPv6 Filtering 54
QoS 55
Add QoS Classification Rules 56
Anti-Attack Settings 58
DNS 59
Dynamic DNS 60
Network Tools 61
Port Mapping 62
IGMP Proxy 63
IGMP Snooping 64
MLD Configuration 65
UPnP 66
DSL 67
Net USB 68
Routing 69
Static Routing 70
IPv6 Static Routing 71
Policy Route 72
RIP 73
RIPng 74
NAT 75
FTPD Setting 76
FTPD Account 77
Management 78
System Management 78
Firmware Update 79
Access Controls 80
Account Password 81
Local Access Control 82
Remote Access Control 83
IP Address 84
Diagnosis 85
DSL Test 86
Traceroute 87
Ping 88
Log Configuration 89
Status 90
Device Info 90
Wireless Clients 91
DHCP Clients 92
Logs 93
Statistics 94
Route Info 95
Help 96

Connecting To Your Wireless Network 97
Windows® 8 97
WPA/WPA2 97
Windows® 7 99
WPA/WPA2 99
WPS 102
Windows Vista® 106
WPA/WPA2 107
WPS/WCN 2.0 109
Windows® XP 110

WPA/WPA2 111

Troubleshooting 113

Wireless Security 117
What is WPA? 117

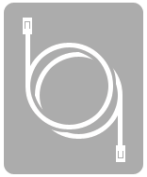
Networking Basics 118
Check your IP address 118
Statically Assign an IP address 119

Link'n Print 120

Technical Specifications 125

Package Contents

Wireless AC Dual-Band ADSL2+ Modem Router



Ethernet Cable

Power Adapter

WI-FI Configuration Note

If any of the above items are missing, please contact your reseller.

Note: *Using a power supply with a different voltage rating than the one included with the Wireless AC Dual-Band ADSL2+ Modem Router will cause damage and void the warranty for this product.*

System Requirements

Network Requirements	• An Ethernet-based Cable or DSL modem • IEEE 802.11ac, 802.11a, 802.11n or 802.11g wireless clients • 10/100 Ethernet
Web-based Configuration Utility Requirements	**Computer with the following:** • Windows®, Macintosh, or Linux-based operating system • An installed Ethernet adapter **Browser Requirements:** Microsoft Internet Explorer® v7, Mozilla® Firefox® v9.0, Google® Chrome 16.0, or Safari® v4 or higher version **Windows® Users:** Make sure you have the latest version of Java installed. Visit www.java.com to download the latest version.

Introduction

The D-Link Wireless AC Dual-Band ADSL2+ Modem Router is a IEEE 802.11ac compliant device that delivers up to 3 times faster speeds than 802.11n while staying backward compatible with 802.11a/g/b devices. Connect the Wireless AC Dual-Band ADSL2+ Modem Router to a Cable or DSL modem and provide high-speed Internet access to multiple computers, game consoles, and media players. Create a secure wireless network to share photos, files, music, videos, printers, and network storage. Powered by the 802.11ac technology this router provides wireless coverage for homes and offices, or for users running bandwidth-intensive applications.

With some routers, all wired and wireless traffic, including VoIP, Video Streaming, Online Gaming, and Web browsing are mixed together into a single data stream. By handling data this way, applications like video streaming could pause or delay. With the D-Link Intelligent QoS Technology, wired and wireless traffic are analyzed and separated into multiple data streams.

The Wireless AC Dual-Band ADSL2+ Modem Router supports the latest wireless security features to help prevent unauthorized access, be it from over a wireless network or the Internet. Support for WPA™ and WPA2™ standards ensure that you will be able to use the best possible encryption regardless of your client devices. In addition, this router utilizes Dual Active Firewalls (SPI and NAT) to prevent potential attacks from across the Internet for the ideal centerpiece for your wireless network in the home or office.

Features

- **Ultimate Fast Wireless Networking** - The Wireless AC Dual-Band ADSL2+ Modem Routerprovides up to 300Mbps wireless connection in 2.4GHz band, 433Mbps wireless connection in 5GHz with other 802.11ac and draft 802.11n wireless clients. This capability allows users to participate in real-time activities online, such as video streaming, online gaming, and real-time audio. The performance of this 802.11ac wireless router gives you the freedom of wireless networking at speeds 3x faster than 802.11n.

- **Compatible with 802.11a/g/n Devices** - The Wireless AC Dual-Band ADSL2+ Modem Router is still fully compatible with the IEEE 802.11a, 802.11g and 802.11n, so it can connect with existing 802.11a, 802.11g and 802.11n PCI, USB, and Cardbus adapters.

- **Advanced Firewall Features** - The Web-based user interface displays a number of advanced network management features including:

    - **Content Filtering** - Easily applied content filtering based on MAC Address, URL, and/or Domain Name.

    - **Filter Scheduling** - These filters can be scheduled to be active on certain days or for a duration of hours or minutes.

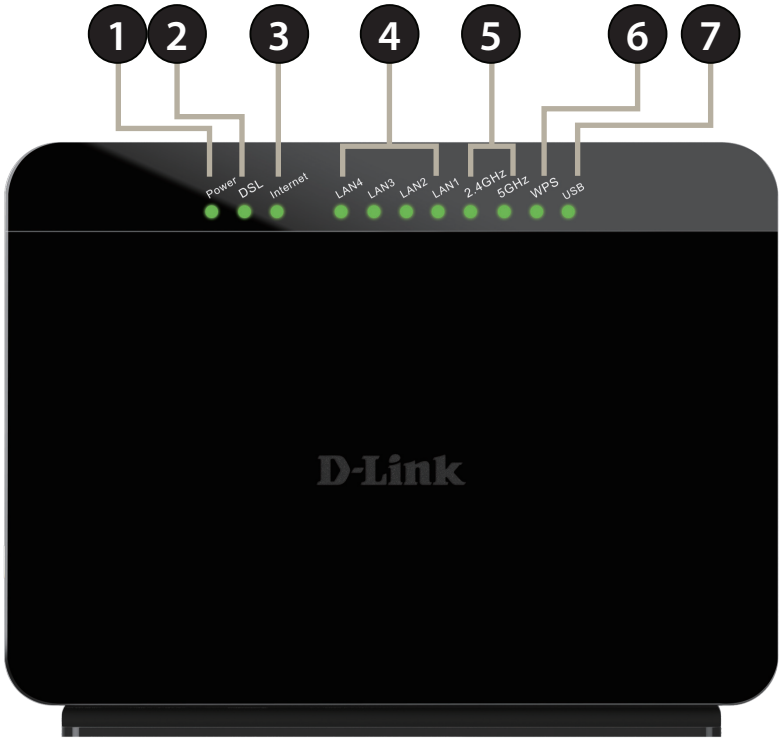
    - **Secure Multiple/Concurrent Sessions** - The Wireless AC Dual-Band ADSL2+ Modem Router can pass through VPN sessions. It supports multiple and concurrent IPSec and PPTP sessions, so users behind the Wireless AC Dual-Band ADSL2+ Modem Router can securely access corporate networks.

- **User-friendly Setup Wizard** - Through its easy-to-use Web-based user interface, the Wireless AC Dual-Band ADSL2+ Modem Router lets you control what information is accessible to those on the wireless network, whether from the Internet or from your company's server. Configure your router to your specific settings within minutes.

* Maximum wireless signal rate derived from IEEE Standard 802.11a, 802.11g, 802.11n and draft 802.11ac specifications. Actual data throughput will vary. Network conditions and environmental factors, including volume of network traffic, building materials and construction, and network overhead, lower actual data throughput rate. Environmental conditions will adversely affect wireless signal range.

Hardware Overview

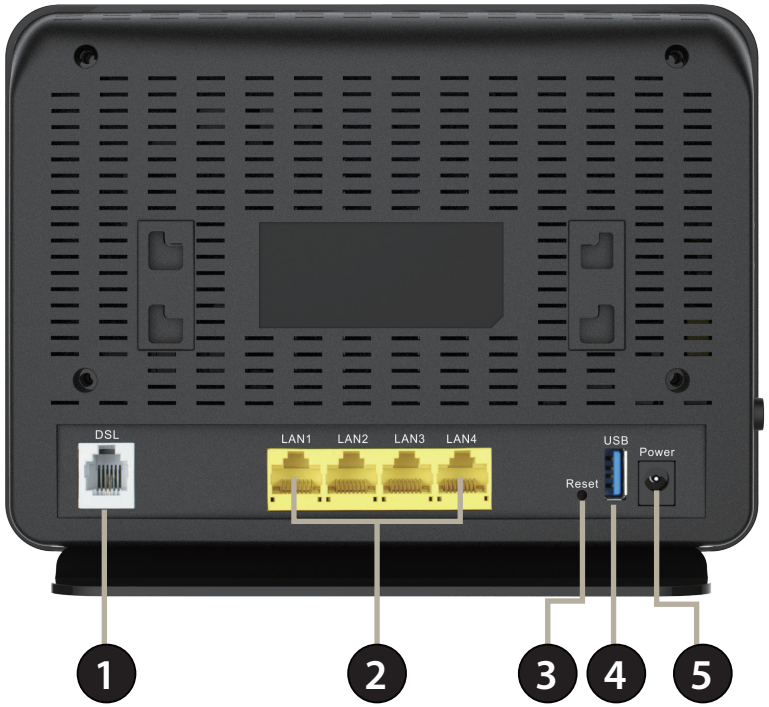
LEDs



1	Power LED	A solid green light indicates a proper connection to the power supply.
2	DSL LED	A solid green light indicates a proper DSL connection.
3	Internet LED	A solid light indicates connection on the Internet port.
4	Local Network LEDs	A solid light indicates a connection to an Ethernet-enabled computer on ports 1-4. This LED blinks during data transmission
5	Wireless LED	A solid light indicates that the wireless networks are ready.
6	WPS LED	This LED blinks during WPS handshake phase.
7	USB LED	A solid green light indicates a USB is connected.

Hardware Overview

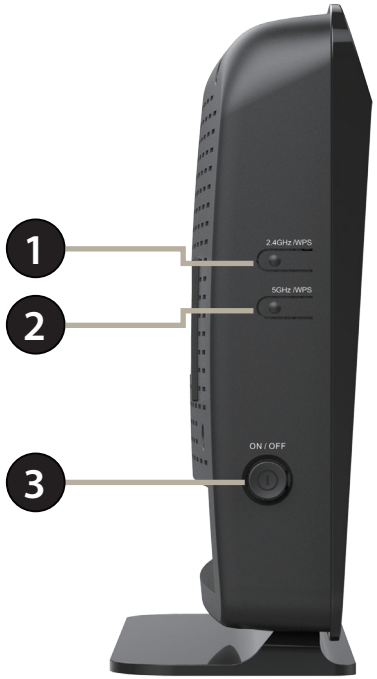
Back



1	Internet/DSL Port	Using an Ethernet cable, connect your broadband modem to this port.
2	LAN Ports (1-4)	Connect 10/100 Ethernet devices such as computers, switches, storage (NAS) devices and game consoles.
3	Reset Button	Insert a paperclip in the hole and wait for several seconds to reset the router to default settings.
4	USB Port	Attaches to a USB 2.0 printer or storage device to share with your network.
5	Power Receptor	Receptor for the supplied power adapter.

Hardware Overview

Left



1	2.4 GHz Wireless	Use this button to initiate a WPS connection on the 2.4 GHz band.
2	5 GHz Wireless	Use this button to initiate a WPS connection on the 5 GHz band.
3	Power	Use this button to power the device on or off.

Installation

This section will walk you through the installation process. Placement of the router is very important. Do not place the router in an enclosed area such as a closet, cabinet, or in the attic or garage.

Before you Begin

- Please configure the router with the computer that was last connected directly to your modem.
- You can only use the Ethernet port on your modem. If you were using the USB connection before using the router, then you must turn off your modem, disconnect the USB cable and connect an Ethernet cable to the Internet port on the router, and then turn the modem back on. In some cases, you may need to call your ISP to change connection types (USB to Ethernet).
- If you have DSL and are connecting via PPPoE, make sure you disable or uninstall any PPPoE software such as WinPoet, Broadjump, or Enternet 300 from your computer or you will not be able to connect to the Internet.

Wireless Basics

D-Link wireless products are based on industry standards to provide easy-to-use and compatible high-speed wireless connectivity within your home, business or public access wireless networks. Strictly adhering to the IEEE standard, the D-Link wireless family of products will allow you to securely access the data you want, when and where you want it. You will be able to enjoy the freedom that wireless networking delivers.

A wireless local area network (WLAN) is a cellular computer network that transmits and receives data with radio signals instead of wires. Wireless LANs are used increasingly in both home and office environments, and public areas such as airports, coffee shops and universities. Innovative ways to utilize WLAN technology are helping people to work and communicate more efficiently. Increased mobility and the absence of cabling and other fixed infrastructure have proven to be beneficial for many users.

Wireless users can use the same applications they use on a wired network. Wireless adapter cards used on laptop and desktop systems support the same protocols as Ethernet adapter cards.

Under many circumstances, it may be desirable for mobile network devices to link to a conventional Ethernet LAN in order to use servers, printers or an Internet connection supplied through the wired LAN. A Wireless Router is a device used to provide this link.

Wireless Installation Considerations

The D-Link wireless router lets you access your network using a wireless connection from virtually anywhere within the operating range of your wireless network. Keep in mind, however, that the number, thickness and location of walls, ceilings, or other objects that the wireless signals must pass through, may limit the range. Typical ranges vary depending on the types of materials and background RF (radio frequency) noise in your home or business. The key to maximizing wireless range is to follow these basic guidelines:

1. Keep the number of walls and ceilings between the D-Link router and other network devices to a minimum - each wall or ceiling can reduce your adapter's range from 3-90 feet (1-30 meters.) Position your devices so that the number of walls or ceilings is minimized.

2. Be aware of the direct line between network devices. A wall that is 1.5 feet thick (.5 meters), at a 45-degree angle appears to be almost 3 feet (1 meter) thick. At a 2-degree angle it looks over 42 feet (14 meters) thick! Position devices so that the signal will travel straight through a wall or ceiling (instead of at an angle) for better reception.

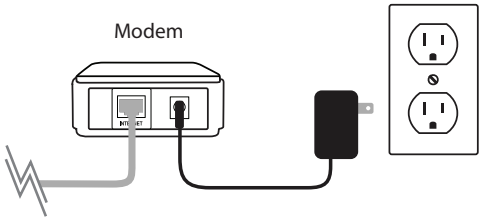
3. Building Materials make a difference. A solid metal door or aluminum studs may have a negative effect on range. Try to position access points, wireless routers, and computers so that the signal passes through drywall or open doorways. Materials and objects such as glass, steel, metal, walls with insulation, water (fish tanks), mirrors, file cabinets, brick, and concrete will degrade your wireless signal.

4. Keep your product away (at least 3-6 feet or 1-2 meters) from electrical devices or appliances that generate RF noise.

5. If you are using 2.4GHz cordless phones or X-10 (wireless products such as ceiling fans, lights, and home security systems), your wireless connection may degrade dramatically or drop completely. Make sure your 2.4GHz phone base is as far away from your wireless devices as possible. The base transmits a signal even if the phone in not in use.

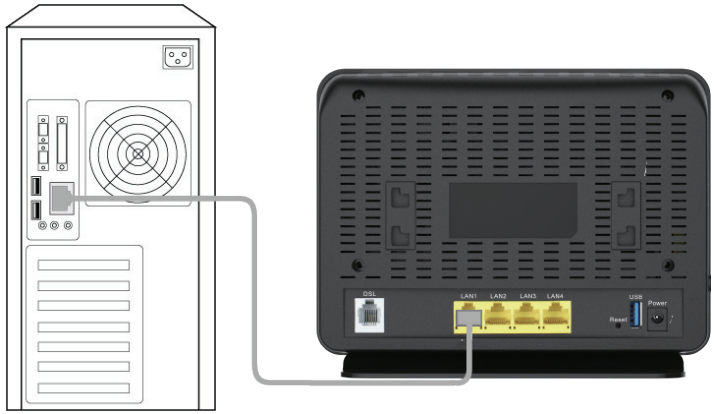
Installation

1. Turn off and unplug your cable or DSL broadband modem. This is required.



2. Position your router close to your modem and a computer. Place the router in an open area of your intended work area for better wireless coverage.

3. Unplug the Ethernet cable from your modem (or existing router if upgrading) that is connected to your computer. Plug it into the LAN port labeled **1** on the back of your router. The router is now connected to your computer.



Computer

GO-DSL-AC750

Connect a Wireless Client to your Router

WPS Button

The easiest and most secure way to connect your wireless devices to the router is WPS (Wi-Fi Protected Setup). Most wireless devices such as wireless adapters, media players, Blu-ray DVD players, wireless printers and cameras will have a WPS button (or a software utility with WPS) that you can press to connect to the GO-DSL-AC750 router. Please refer to your user manual for the wireless device you want to connect to make sure you understand how to enable WPS. Once you know, follow the steps below:

Step 1 - Press the WPS button on the side of GO-DSL-AC750 for about 1 second. The Internet LED on the front will start to blink.

Step 2 - Within 2 minutes, press the WPS button on your wireless client (or launch the software utility and start the WPS process).

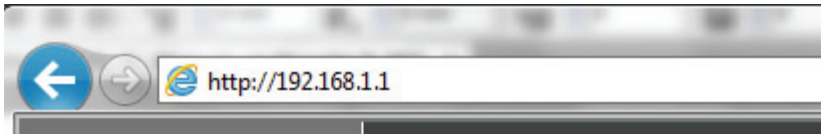
Step 3 - Allow up to 1 minute to configure. Once the Internet light stops blinking, you will be connected and your wireless connection will be secure with WPA2.

Configuration
Web-based Configuration Utility

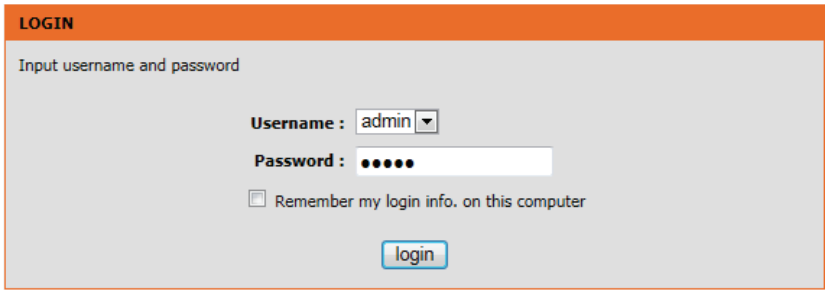
This section will show you how to configure your D-Link wireless access point using the web-based configuration utility.

If you wish to change the default settings or adjust the configuration of the GO-DSL-AC750 you may use the web-based configuration utility.

To access the configuration utility, open a web browser such as Internet Explorer and enter **http://192.168.1.1** in the address field.



Select **admin** from the drop-down menu and then enter your password. The default password is **admin**. You will be directed to the **Setup Wizard** page.



This wizard is designed to guide you through a step-by-step process to configure your new D-Link router and connect to the Internet.

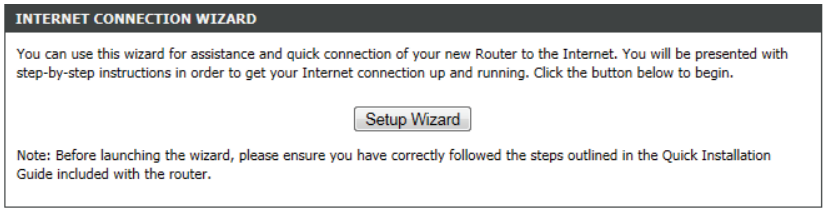
Click the **Setup Wizard** button to continue.

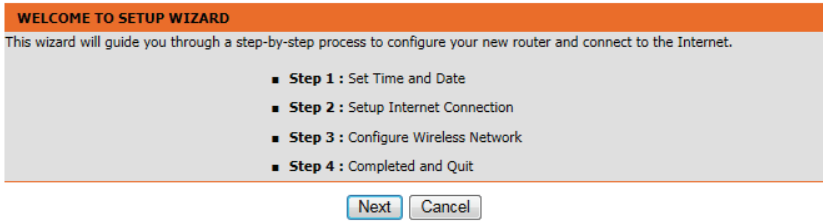
Setup Wizard

Click **Setup Wizard** to configure your router.

If you want to configure the access point manually without running the wizard, skip to "Manual Configuration" on page 20.

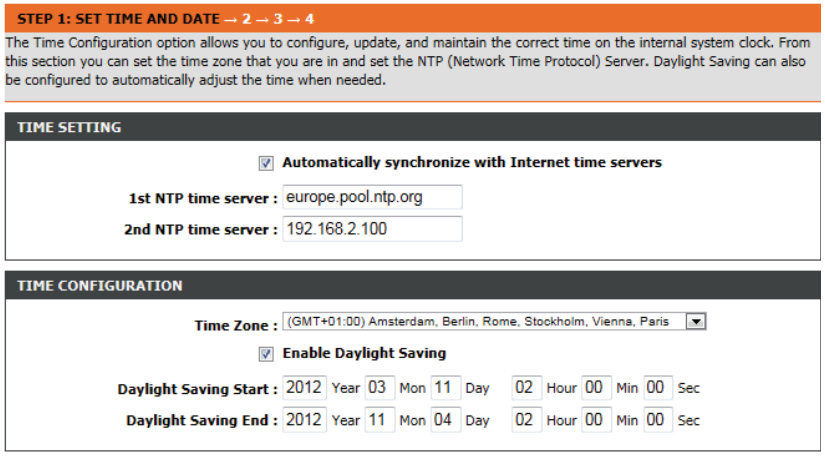
Click **Next** to continue.


INTERNET CONNECTION WIZARD
You can use this wizard for assistance and quick connection of your new Router to the Internet. You will be presented with step-by-step instructions in order to get your Internet connection up and running. Click the button below to begin.
Setup Wizard
Note: Before launching the wizard, please ensure you have correctly followed the steps outlined in the Quick Installation Guide included with the router.


WELCOME TO SETUP WIZARD
This wizard will guide you through a step-by-step process to configure your new router and connect to the Internet.
Step 1 : Set Time and Date
Step 2 : Setup Internet Connection
Step 3 : Configure Wireless Network
Step 4 : Completed and Quit
Next
Cancel

This section of the wizard enables you to use an international time server to set the internal time and date for the router.

Automatically Synchronize: Enable or disable automatic synchronisation with an Internet Time Server.
1st NTP Time Server: Specify an address for the primary Internet Time Server.
2nd NTP Time Server: Specify an address for the secondary Internet Time Server.
Time Zone: Select your time zone from the drop down menu.
Enable Daylight Saving: Enable or disable daylight saving.
Daylight Saving Start/End: Specify the time and date when daylight saving should start/end.


STEP 1: SET TIME AND DATE → 2 → 3 → 4
The Time Configuration option allows you to configure, update, and maintain the correct time on the internal system clock. From this section you can set the time zone that you are in and set the NTP (Network Time Protocol) Server. Daylight Saving can also be configured to automatically adjust the time when needed.
TIME SETTING
Automatically synchronize with Internet time servers
1st NTP time server : europe.pool.ntp.org
2nd NTP time server : 192.168.2.100
TIME CONFIGURATION
Time Zone : (GMT+01:00) Amsterdam, Berlin, Rome, Stockholm, Vienna, Paris
Enable Daylight Saving
Daylight Saving Start : 2012 Year 03 Mon 11 Day 02 Hour 00 Min 00 Sec
Daylight Saving End : 2012 Year 11 Mon 04 Day 02 Hour 00 Min 00 Sec

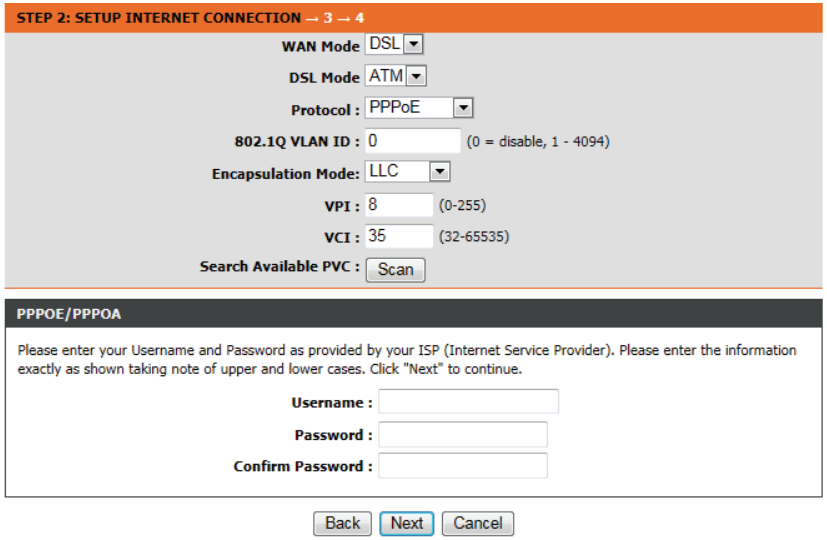
This section of the wizard enables you to configure your internet connection type. Select the appropriate wan connection type which is provided by your ISP.

If the router detected or you selected **PPPoE**, enter your PPPoE username and password and click **Next** to continue.

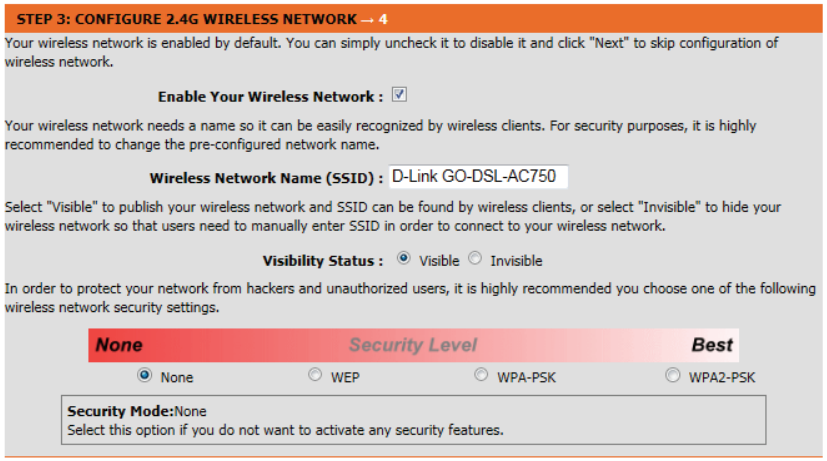
Note: *Make sure to remove your PPPoE software from your computer. The software is no longer needed and will not work through a router.*

If the router detected or you selected **PPTP**, enter your PPTP username, password, and other information supplied by your ISP. Click **Next** to continue.

If the router detected or you selected **L2TP**, enter your L2TP username, password, and other information supplied by your ISP. Click **Next** to continue.


STEP 2: SETUP INTERNET CONNECTION → 3 → 4
WAN Mode DSL
DSL Mode ATM
Protocol : PPPoE
802.1Q VLAN ID : 0 (0 = disable, 1 - 4094)
Encapsulation Mode: LLC
VPI : 8 (0-255)
VCI : 35 (32-65535)
Search Available PVC : Scan
PPPOE/PPPOA
Please enter your Username and Password as provided by your ISP (Internet Service Provider). Please enter the information exactly as shown taking note of upper and lower cases. Click "Next" to continue.
Username :
Password :
Confirm Password :
Back
Next
Cancel

This section of the wizard enables you to configure your 2.4G wireless connection. You can also configure the wireless network and security settings. If you prefer not to, uncheck the **Enable Your Wireless Network** box.

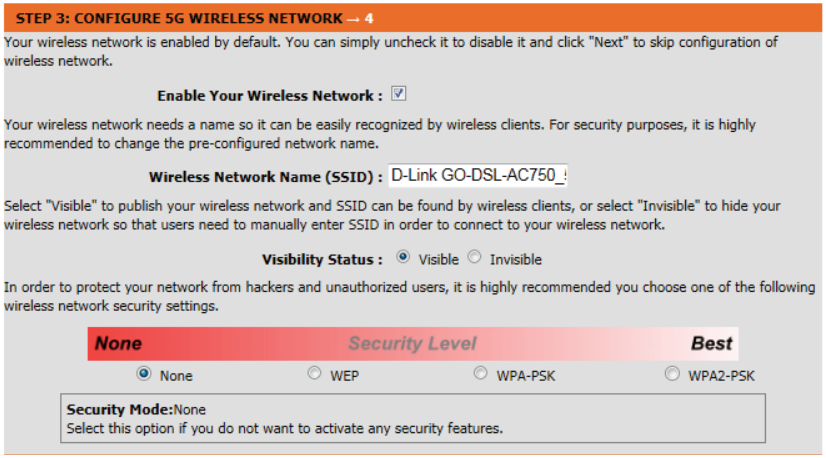

STEP 3: CONFIGURE 2.4G WIRELESS NETWORK → 4
Your wireless network is enabled by default. You can simply uncheck it to disable it and click "Next" to skip configuration of wireless network.
Enable Your Wireless Network :
Your wireless network needs a name so it can be easily recognized by wireless clients. For security purposes, it is highly recommended to change the pre-configured network name.
Wireless Network Name (SSID) : D-Link GO-DSL-AC750
Select "Visible" to publish your wireless network and SSID can be found by wireless clients, or select "Invisible" to hide your wireless network so that users need to manually enter SSID in order to connect to your wireless network.
Visibility Status : Visible Invisible
In order to protect your network from hackers and unauthorized users, it is highly recommended you choose one of the following wireless network security settings.
None
Security Level
Best
None
WEP
WPA-PSK
WPA2-PSK
Security Mode:None
Select this option if you do not want to activate any security features.

Choose a network name for your wireless network, and choose if you wish to make the wireless network **visible** or **invisible**.

It is highly recomended to secure your wireless network. Select from the available options. For more information see “Wireless Security” on page 117.

Click **Next** to continue.

This section of the wizard enables you to configure your 5G wireless connection. You can also configure the wireless network and security settings. If you prefer not to, uncheck the **Enable Your Wireless Network** box.


STEP 3: CONFIGURE 5G WIRELESS NETWORK → 4
Your wireless network is enabled by default. You can simply uncheck it to disable it and click "Next" to skip configuration of wireless network.
Enable Your Wireless Network :
Your wireless network needs a name so it can be easily recognized by wireless clients. For security purposes, it is highly recommended to change the pre-configured network name.
Wireless Network Name (SSID) : D-Link GO-DSL-AC750_
Select "Visible" to publish your wireless network and SSID can be found by wireless clients, or select "Invisible" to hide your wireless network so that users need to manually enter SSID in order to connect to your wireless network.
Visibility Status : Visible Invisible
In order to protect your network from hackers and unauthorized users, it is highly recommended you choose one of the following wireless network security settings.
None
Security Level
Best
None
WEP
WPA-PSK
WPA2-PSK
Security Mode:None
Select this option if you do not want to activate any security features.

Choose a network name for your wireless network, and choose if you wish to make the wireless network **visible** or **invisible**.

It is highly recomended to secure your wireless network. Select from the available options. For more information see “Wireless Security” on page 117.

Click **Next** to continue.

Your router is now setup.

A summary page will be displayed, showing the current settings for your WAN, 2.4 GHz and 5 GHz wireless networks. It is recommended that you make a note of this information for future reference.

Click **Finish** to save your network settings.

In order for your network settings to take effect the AP will reboot automatically.

When the device has finished rebooting the main screen will display.

STEP 4: SAVE AND APPLY CHANGES

Setup complete. Click "Back" to review or modify settings.

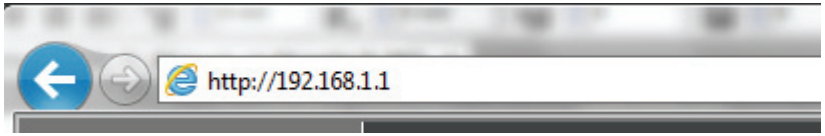
If your Internet connection does not work, you can try the Setup Wizard again with alternative settings or use Manual Setup instead if you have your Internet connection details as provided by your ISP.

Below is a detailed summary of your settings. Please print this page out, or write the information on a piece of paper, so you can configure the correct settings on your wireless client adapters.

Time Settings :	1
NTP Server 1 :	europe.pool.ntp.org
NTP Server 2 :	192.168.2.100
Time Zone :	CET
Daylight Saving Time :	1
VPI / VCI :	8/35
Protocol :	PPPoE
Connection Type :	LLC
802.1Q VLAN ID :	0
Priority :	0
Username :	d-link
Password :	*****
SSID (2.4G):	D-Link GO-DSL-AC750
Visibility Status :	Visible
Encryption :	None
Pre-Shared Key :	N/A
WEP Key :	N/A
SSID (5G) :	D-Link GO-DSL-AC750_5G
Visibility Status (5G) :	Visible
Encryption (5G) :	None
Pre-Shared Key (5G) :	N/A
WEP Key (5G) :	N/A

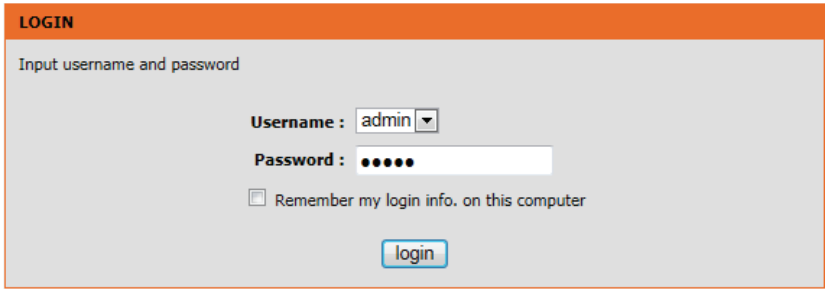
Manual Configuration
Setup

If you wish to change the default settings or adjust the configuration of the GO-DSL-AC750 you may use the web-based configuration utility. To access the configuration utility, open a web-browser such as Internet Explorer and enter address of the router (**http://192.168.1.1**).



Non-Windows and Non-Mac users may also connect by typing **http://192.168.1.1** in the address bar.

Select **admin** from the drop-down menu and then enter your password. The default password is **admin**.

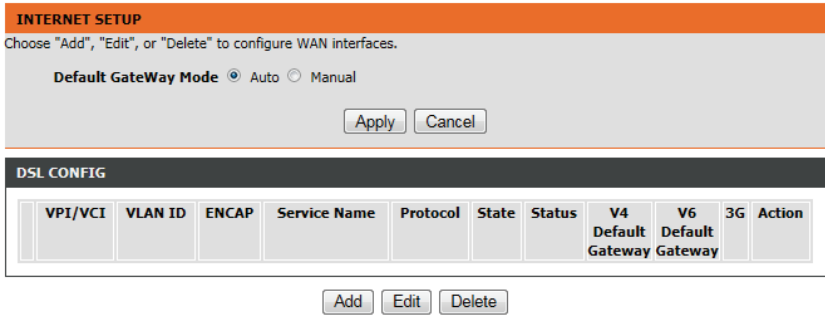


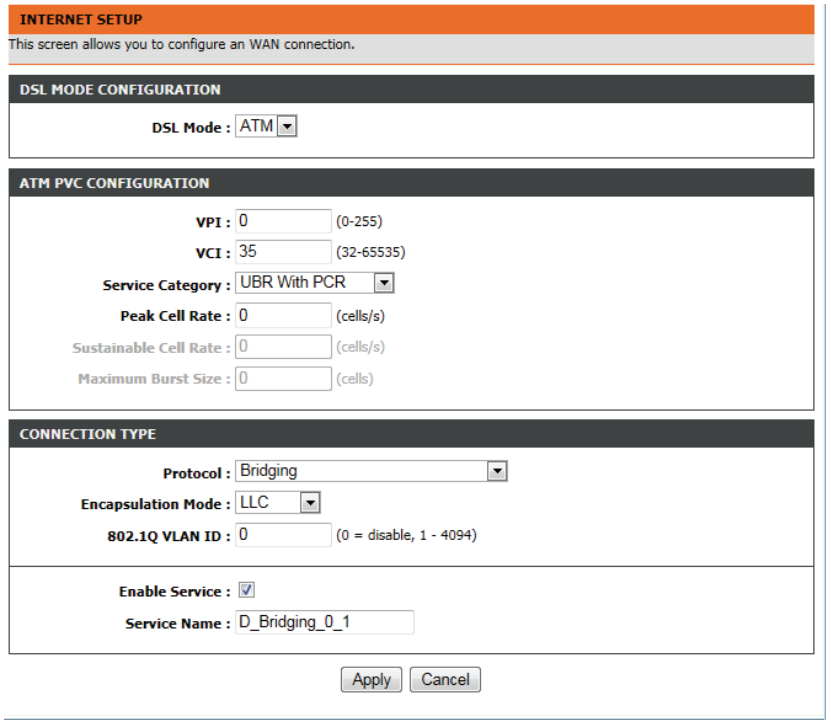
Internet Setup

Click **Internet Setup** on the left menu to configure your connection manually.

If you want to configure your router to connect to the Internet using the wizard, click **Wizard** on the left menu and you will be directed to the Quick Setup Wizard.

Click the **Add** button to reveal the DSL configuration options .




INTERNET SETUP
This screen allows you to configure an WAN connection.
DSL MODE CONFIGURATION
DSL Mode : ATM
ATM PVC CONFIGURATION
VPI : 0 (0-255)
VCI : 35 (32-65535)
Service Category : UBR With PCR
Peak Cell Rate : 0 (cells/s)
Sustainable Cell Rate : 0 (cells/s)
Maximum Burst Size : 0 (cells)
CONNECTION TYPE
Protocol : Bridging
Encapsulation Mode : LLC
802.1Q VLAN ID : 0 (0 = disable, 1 - 4094)
Enable Service :
Service Name : D_Bridging_0_1
Apply
Cancel

The following parameters will be available for configuration:

VPI: Virtual path identifier (VPI) is the virtual path between two points in an ATM network. Its valid value is between 0 and 255. Enter the correct VPI provided by your ISP. By default, VPI is set to 1.

VCI: Virtual channel identifier (VCI) is the virtual channel between two points in an ATM network. Its valid value is between 1 and 65535. Enter the correct VCI provided by your ISP. By default, VCI is set to 32.

Service Category: Select the Quality of Service types for this Virtual Circuit. The ATM QoS types include CBR (Constant Bit Rate), VBR (Variable Bit Rate) and UBR (Unspecified Bit Rate). These QoS types are all controlled by the parameters specified below, including PCR, SCR and MBS.

Peak Cell Rate: Peak cell rate (PCR) is the maximum rate at which cells can be transmitted along a connection in the ATM network.

Sustainable Cell Rate: Sustainable cell rate (SCR) is the maximum rate that traffic can pass over PVC without the risk of cell loss.

Maximum Burst Size: Maximum burst size (MBS) is the maximum number of cells that can be transmitted at the PCR.

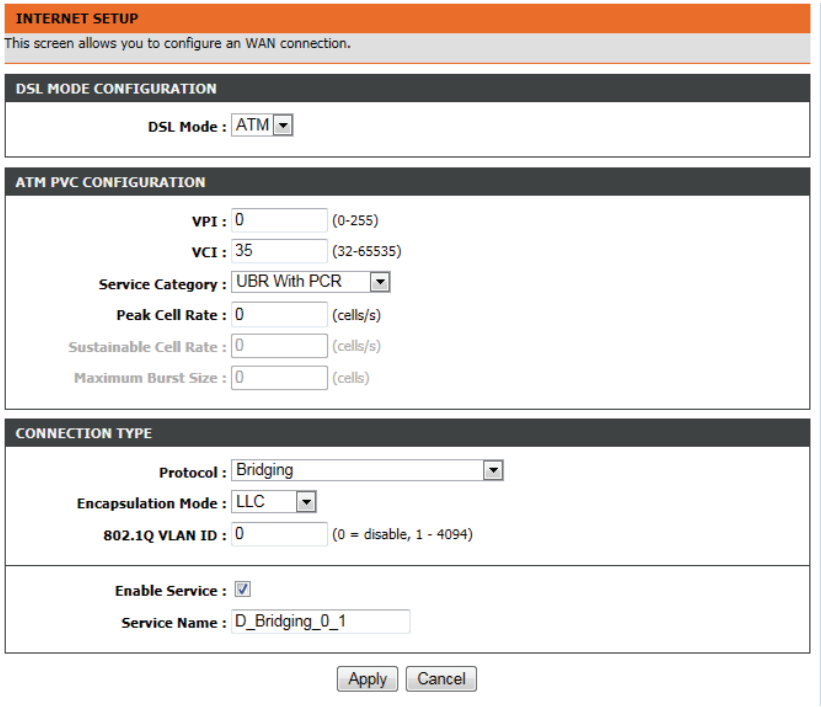
Protocol: Select the appropriate protocol from the drop-down menu.

Encapsulation Mode: You can select LLC or VCMUX. In this example, the encapsulation mode is set to LLC.

802.1Q VLAN ID: Select this option to Activate/Deactivate the 4094 VID on the 4 different queues. VID (VLAN ID) is the identification of the VLAN, which is basically used by the standard 802.1Q. It has 12 bits and allows the identification of 4096 (2^12) VLANs. Of the 4096 possible VIDs, a VID of 0 is used to identify priority frames and value 4095 (FFF) is reserved, so the maximum possible VLAN configurations are 4,094

Enable Service: Choose to enable or disable the service.

Service Name: Enter a name for the service.


INTERNET SETUP
This screen allows you to configure an WAN connection.
DSL MODE CONFIGURATION
DSL Mode : ATM
ATM PVC CONFIGURATION
VPI : 0 (0-255)
VCI : 35 (32-65535)
Service Category : UBR With PCR
Peak Cell Rate : 0 (cells/s)
Sustainable Cell Rate : 0 (cells/s)
Maximum Burst Size : 0 (cells)
CONNECTION TYPE
Protocol : Bridging
Encapsulation Mode : LLC
802.1Q VLAN ID : 0 (0 = disable, 1 - 4094)
Enable Service :
Service Name : D_Bridging_0_1
Apply
Cancel

Click **Apply** to save your Internet Setup settings.

2.4G Wireless

On this page the user can configure the Wireless settings for this device. There are 2 options to configure 2.4G Wireless Settings. Firstly, the user can choose to make use of the **Wireless Basic** settings. Secondly, the user can choose to make use **Wireless Security** settings.

Click the **Wireless Basic** button to view the basic wireless configuration options .

WIRELESS SETTINGS -- WIRELESS BASIC
Configure your wireless basic settings.
Wireless Basic
WIRELESS SETTINGS -- WIRELESS SECURITY
Configure your wireless security settings.
Wireless Security

Enable Wireless: Choose to enable or disable the wireless networks.

AP Isolate: Choose to enable or disable wireless isolation.

SSID: Enter an SSID for the wireless network.

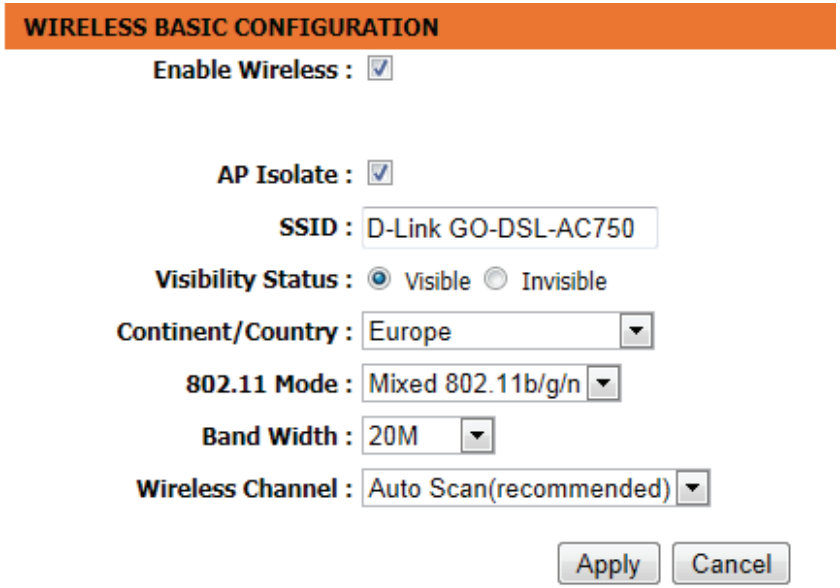
Visisbility Status: Choose to enable SSID broadcast so other wireless devices can find the network.

Continent/Country: Depending on what country the router is used in, regulations provide for the router to automatically set the transmit power and frequencies that may be used in that country.

802.11 Mode: Select from the dropdown menu the mode of operation you require.

Bandwidth: Use the dropdown menu to select the channel bandwidth.

Wireless Channel: Use the dropdown menu to select a wireless channel, or let the router scan automatically.



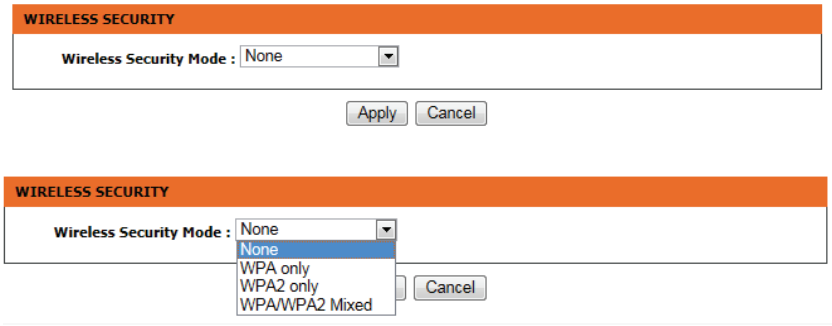
2.4G Wireless Security

Wireless security helps to prevent unauthorized users from accessing your wireless network, or seeing data being passed between the router and wireless clients. The GO-DSL-AC750 supports two popular wireless security protocols, you should select a protocol based on the wireless clients which will be accessing your network.

Wired Equivalent Privacy (WEP) - This is an older form of wireless security and should only be used if your wireless clients do not support the newer WPA or WPA2 protocols.

Wi-Fi Protected Access (WPA/WPA2) - This is a newer and more secure protocol for wireless security. It uses a cipher combined with a pre-shared key (password) to encrypt data being sent over the wireless network. It is recommended that you use this security method if it is supported by your wireless clients.

Wireless Security Mode: Select a wireless security encryption option. You can also choose to not use one by selecting **None**, but this is not recommended.



5G Wireless

On this page the user can configure the Wireless settings for this device. There are 2 options to configure 5G Wireless Settings. Firstly, the user can choose to make use of the **Wireless Basic** settings. Secondly, the user can choose to make use **Wireless Security** settings.

Click the **Wireless Basic** button to view the basic wireless configuration options .

WIRELESS SETTINGS -- WIRELESS BASIC
Configure your wireless basic settings.
Wireless Basic
WIRELESS SETTINGS -- WIRELESS SECURITY
Configure your wireless security settings.
Wireless Security

Enable Wireless: Choose to enable or disable the wireless networks.

AP Isolate: Choose to enable or disable wireless isolation.

SSID: Enter an SSID for the wireless network.

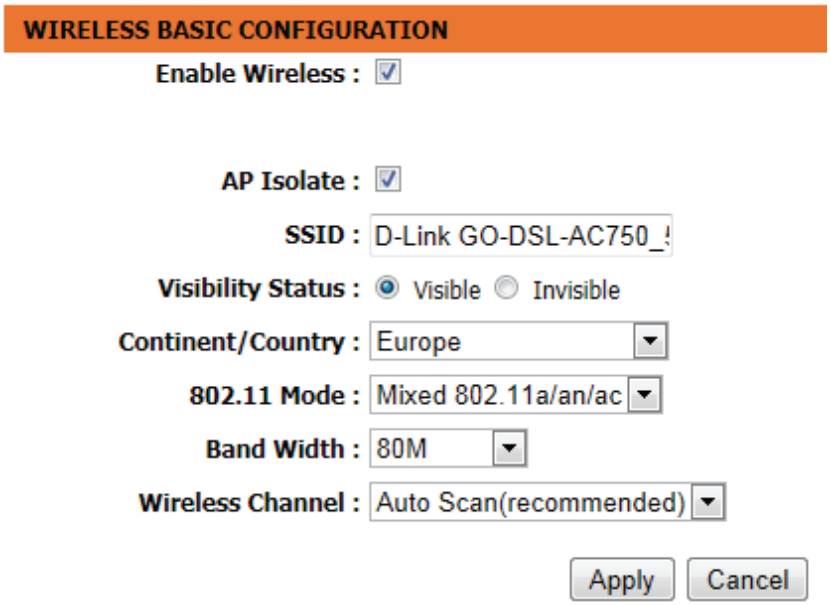
Visibility Status: Choose to enable SSID broadcast so other wireless devices can find the network.

Continent/Country: Depending on what country the router is used in, regulations provide for the router to automatically set the transmit power and frequencies that may be used in that country.

802.11 Mode: Select from the dropdown menu the mode of operation you require.

Bandwidth: Use the dropdown menu to select the channel bandwidth.

Wireless Channel: Use the dropdown menu to select a wireless channel, or let the router scan automatically.

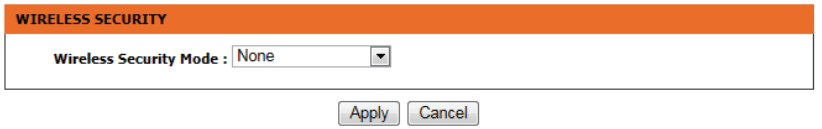


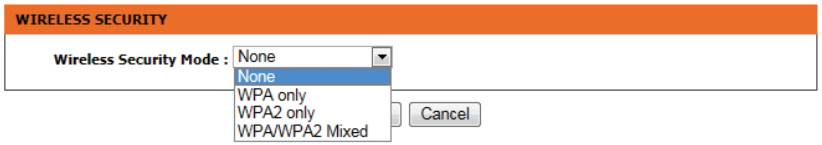
5G Wireless Security

Wireless security helps to prevent unauthorized users from accessing your wireless network, or seeing data being passed between the router and wireless clients. The GO-DSL-AC750 supports two popular wireless security protocols, you should select a protocol based on the wireless clients which will be accessing your network.

Wi-Fi Protected Access (WPA/WPA2) - This is a newer and more secure protocol for wireless security. It uses a cipher combined with a pre-shared key (password) to encrypt data being sent over the wireless network. It is recommended that you use this security method if it is supported by your wireless clients.

Wireless Security Mode: Select a wireless security encryption option. You can also choose to not use one by selecting **None**, but this is not recommended.

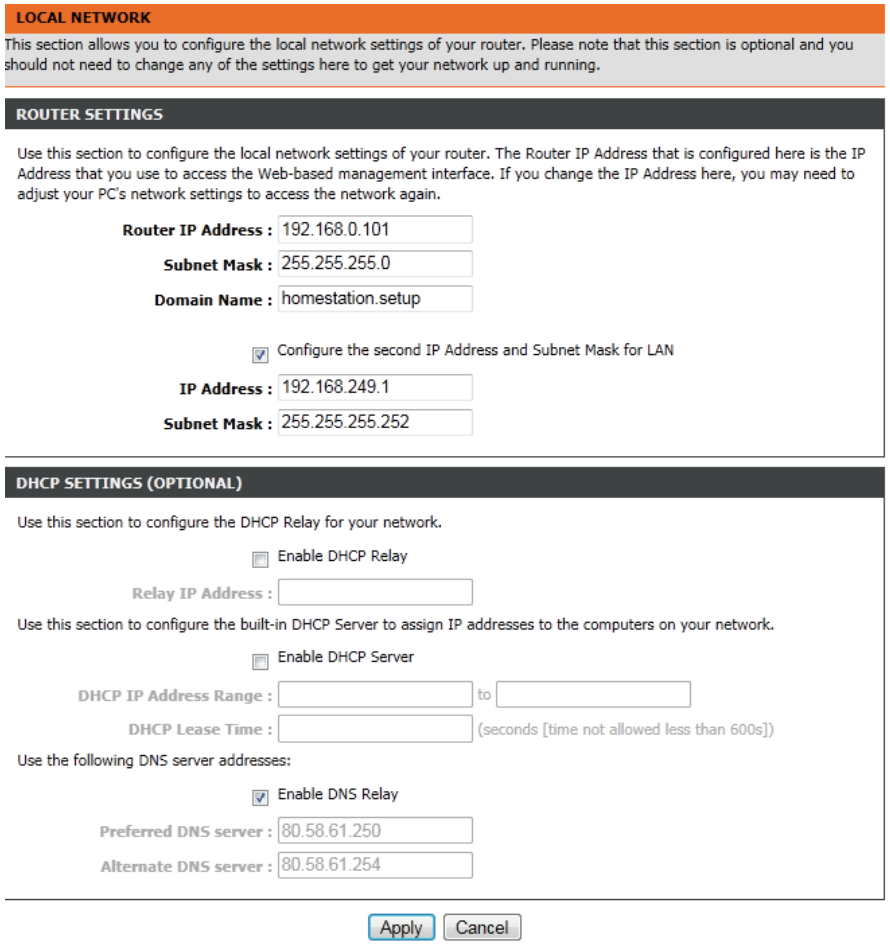




Local Network

When configuring the router for the first time, we recommend that you click use the **Internet Connection Setup Wizard**, and follow the instructions on the screen. This wizard is designed to assist user with a quick and easy method to configure the Internet Connectivity of this router.

Anytime during the Internet Connection Setup Wizard, the user can click on the **Cancel** button to discard any changes made and return to the main page.


LOCAL NETWORK
This section allows you to configure the local network settings of your router. Please note that this section is optional and you should not need to change any of the settings here to get your network up and running.
ROUTER SETTINGS
Use this section to configure the local network settings of your router. The Router IP Address that is configured here is the IP Address that you use to access the Web-based management interface. If you change the IP Address here, you may need to adjust your PC's network settings to access the network again.
Router IP Address : 192.168.0.101
Subnet Mask : 255.255.255.0
Domain Name : homestation.setup
Configure the second IP Address and Subnet Mask for LAN
IP Address : 192.168.249.1
Subnet Mask : 255.255.255.252
DHCP SETTINGS (OPTIONAL)
Use this section to configure the DHCP Relay for your network.
Enable DHCP Relay
Relay IP Address :
Use this section to configure the built-in DHCP Server to assign IP addresses to the computers on your network.
Enable DHCP Server
DHCP IP Address Range : to
DHCP Lease Time : (seconds [time not allowed less than 600s])
Use the following DNS server addresses:
Enable DNS Relay
Preferred DNS server : 80.58.61.250
Alternate DNS server : 80.58.61.254
Apply
Cancel

Router IP Address: Enter the IP address of LAN interface. It is recommended to use an address from a block reserved for private use. This address block is 192.168.1.1- 192.168.255.254.

Subnet Mask: Enter the subnet mask of LAN interface. The range of subnet mask is from 255.255.0.0 to 255.255.255.254.

Domain Name: Enter a domain to be used as a static host name.

Check "**Configure the second IP Address and Subnet Mask for LAN**" to enable a local alias IP address if required.

IP Address: Enter the alias IP address.

Subnet Mask: Enter the alias subnet mask.

Enable DHCP Relay: You can choose Disabled, Enabled or Relay. If set to DHCP Server, the router can assign IP addresses, IP default gateway and DNS Servers to the host under Windows95, Windows NT and other operation systems that support the DHCP client.

Relay IP Address: Enter the desired DHCP relay IP address.

Enable DHCP Server: Enable or disable the DHCP server function.

DHCP IP Address Range: Enter the range of IP addresses the DHCP server can issue from.

DHCP Lease Time: The lease time determines the period that the host retains the assigned IP addresses before the IP addresses change. The default is 259200 seconds.

Enable DNS Relay: If disabled the router will accept the first received DNS assignment from one of the PPPoA, PPPoE or MER enabled PVC(s) during the initial connection setup. If enabled you can enter the IP addresses for primary and secondary DNS servers.

Preferred DNS Server: Enter an address for a preferred DNS Server.

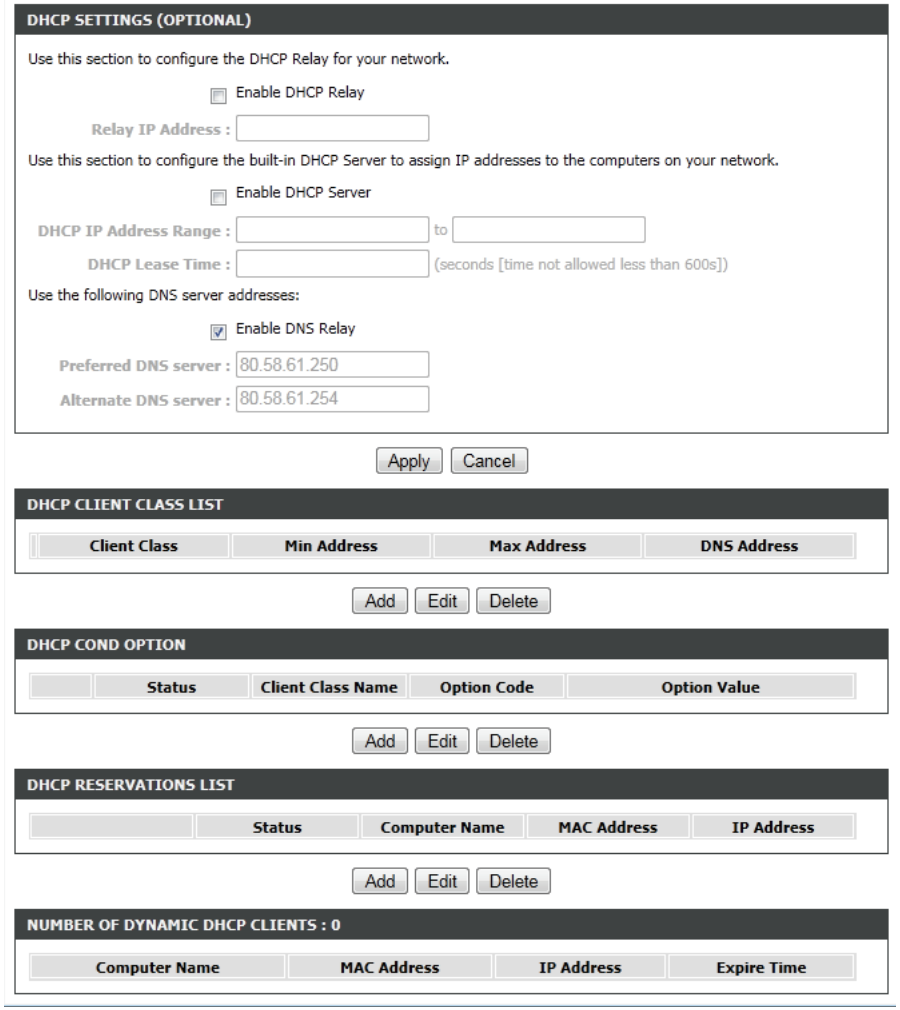
Alternate DNS Server: Enter an address for an alternate DNS Server.

DHCP Client Class List: Client-class processing enables the DHCP server to assign the client an address from a matching scope.

DHCP Conditional Option: Specify the conditions for DHCP class handling.

DHCP Reservations List: Use this option to reserve specific IP Addresses.

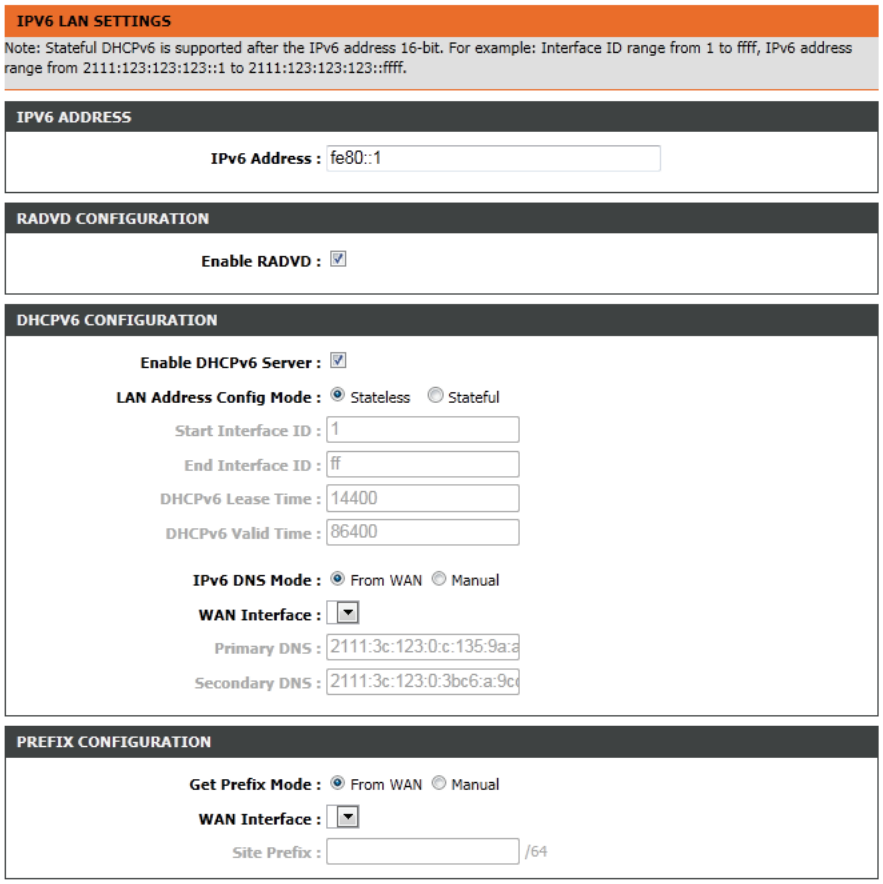
Number of Dynamic DHCP clients: Dynamic DHCP clients will be listed here with supporting information.



Local IPv6 Network

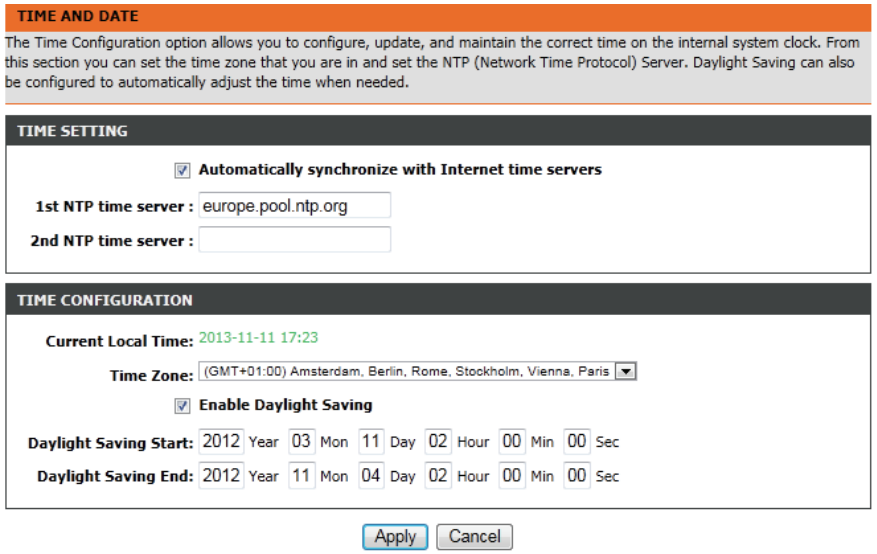
This section enables you to specify various IPv6 settings.

IPv6 Address: Use this option to specify a static IPv6 Address.
Enable RADVD: Enable or disable the Router Advertisement Daemon
Enable DHCPv6 Server: Enable or disable the DHCPv6 server function.
Lan Address Config Mode: Select either stateless (host requests) or stateful (server provisions) LAN IPv6 addressing.
Start/End Interface ID: Enter the range of IP addresses the DHCPv6 server can issue from.
DHCPv6 Lease Time: The lease time determines the period that the host retains the assigned IP addresses before the IP addresses change.
DHCPv6 Valid Time: Specify the period for which an assigned IPv6 address remains valid.
IPv6 DNS Mode: Allow the router to accept the first received IPv6 DNS assignment from a WAN connection. Alternatively, you can manually enter the IP addresses for primary and secondary IPv6 DNS servers.
WAN Interface: Specify the WAN interface to be used.
Primary DNS: Enter an address for a preferred DNS Server.
Secondary DNS: Enter an address for an alternate DNS Server.
Get Prefix Mode: Use this option to specify whether IPv6 Prefix delegation is assigned manually or via a WAN interface.
WAN Interface: Specify the WAN interface to be used. for IPv6 prefix delegation.
Site Prefix: Manually assign an IPv6 prefix delegation.


IPV6 LAN SETTINGS
Note: Stateful DHCPv6 is supported after the IPv6 address 16-bit. For example: Interface ID range from 1 to ffff, IPv6 address range from 2111:123:123:123::1 to 2111:123:123:123::ffff.
IPV6 ADDRESS
IPv6 Address : fe80::1
RADVD CONFIGURATION
Enable RADVD :
DHCPV6 CONFIGURATION
Enable DHCPv6 Server :
LAN Address Config Mode : Stateless Stateful
Start Interface ID : 1
End Interface ID : ff
DHCPv6 Lease Time : 14400
DHCPv6 Valid Time : 86400
IPv6 DNS Mode : From WAN Manual
WAN Interface :
Primary DNS : 2111:3c:123:0:c:135:9a:a
Secondary DNS : 2111:3c:123:0:3bc6:a:9c
PREFIX CONFIGURATION
Get Prefix Mode : From WAN Manual
WAN Interface :
Site Prefix : /64

Time and Date

This section enables you to use an international time server to set the internal time and date for the router.


TIME AND DATE
The Time Configuration option allows you to configure, update, and maintain the correct time on the internal system clock. From this section you can set the time zone that you are in and set the NTP (Network Time Protocol) Server. Daylight Saving can also be configured to automatically adjust the time when needed.
TIME SETTING
Automatically synchronize with Internet time servers
1st NTP time server : europe.pool.ntp.org
2nd NTP time server :
TIME CONFIGURATION
Current Local Time: 2013-11-11 17:23
Time Zone: (GMT+01:00) Amsterdam, Berlin, Rome, Stockholm, Vienna, Paris
Enable Daylight Saving
Daylight Saving Start: 2012 Year 03 Mon 11 Day 02 Hour 00 Min 00 Sec
Daylight Saving End: 2012 Year 11 Mon 04 Day 02 Hour 00 Min 00 Sec
Apply
Cancel

Automatically Synchronize: Enable or disable automatic synchronisation with an Internet Time Server.

1st NTP Time Server: Specify an address for the primary Internet Time Server.

2nd NTP Time Server: Specify an address for the secondary Internet Time Server.

Time Zone: Select the appropriate time zone for your location. This information is required to configure the time-based options for the router.

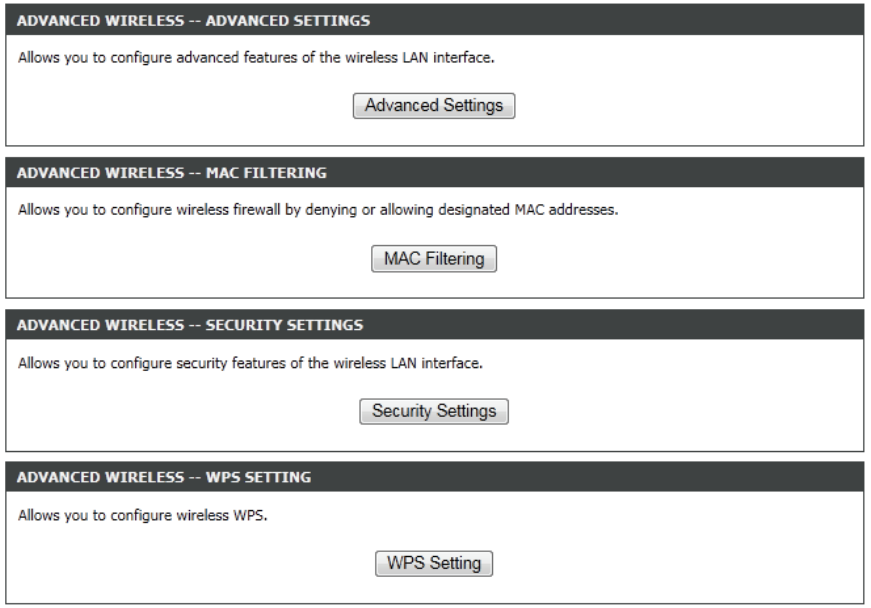
Enable Daylight Saving: Enable or disable daylight saving.

Daylight Saving Start/End: Specify the time and date when daylight saving should start/end.

Advanced

2.4G Advanced Wireless

This section enables you to fine tune the wireless settings on the 2.4G wireless band.


ADVANCED WIRELESS -- ADVANCED SETTINGS
Allows you to configure advanced features of the wireless LAN interface.
Advanced Settings
ADVANCED WIRELESS -- MAC FILTERING
Allows you to configure wireless firewall by denying or allowing designated MAC addresses.
MAC Filtering
ADVANCED WIRELESS -- SECURITY SETTINGS
Allows you to configure security features of the wireless LAN interface.
Security Settings
ADVANCED WIRELESS -- WPS SETTING
Allows you to configure wireless WPS.
WPS Setting

Advanced Settings

Enable Wireless: Choose to enable or disable the wireless networks.

Transmit Power: Set the transmit power of the antennas in pecentage.

Beacon Period: Beacon Interval range can be set from 20 to 1000.

RTS Threshold: This value should remain at its default setting of 2346. If inconsistent data flow is a problem, only a minor modification should be made.

Fragmentation Threshold: The fragmentation threshold, which is specified in bytes, determines whether packets will be fragmented. Packets exceeding the 2346 byte setting will be fragmented before transmission. 2346 is the default setting..

DTIM Interval: DTIM range can be set from 1 to 255. A delivery traffic indication message is a kind of traffic indication message (TIM) which informs the clients of the presence of buffered multicast/broadcast data on the access point.

Preamble Type: Use the dropdown menu to specify whether the Router should use the Short Preamble or Long Preamble type. The preamble type defines the length of the CRC (Cyclic Redundancy Check) block for communication between the Router and roaming wireless adapters

SSID: Enter an SSID for the wireless network.

Visibility Status: Enable the wireless network to be Visible or Invisible to wireless clients. If Invisible, the SSID of the GO-DSL-AC750 will not be seen by site survey utilities, so wireless clients will have to manually enter the SSID of your wireless network in order to connect to it.

User Isolation: Choose to enable or disable wireless user isolation.

Disable WMM Advertise: Enable or Disable WiFi MultiMedia QoS.

Max Clients: Use this option to specify the maximum number of clients.

ADVANCED SETTINGS
Enable wireless
ADVANCED WIRELESS SETTINGS
Transmit Power : 100%
Beacon Period : 100 (20 ~ 1023)
RTS Threshold : 2346 (1 ~ 2347)
Fragmentation Threshold : 2346 (256 ~ 2346)
DTIM Interval : 10 (1 ~ 255)
Preamble Type : long
SSID
SSID: D-Link GO-DSL-AC750
Visibility Status : Visible Invisible
User Isolation : Off
Disable WMM Advertise : On
Max Clients : 16 (1 ~ 32)
GUEST/VIRTUAL ACCESS POINT-1
Enable
Guest SSID : D-Link GO-DSL-AC7502
Visibility Status : Visible Invisible
User Isolation : On
Disable WMM Advertise : On
Max Clients : 32 (1 ~ 32)
GUEST/VIRTUAL ACCESS POINT-2
Enable
Guest SSID : D-Link GO-DSL-AC7503
Visibility Status : Visible Invisible
User Isolation : On
Disable WMM Advertise : On
Max Clients : 32 (1 ~ 32)

Enable Guest Virtual Access Point 1/2/3: Enable or disable a guest network.

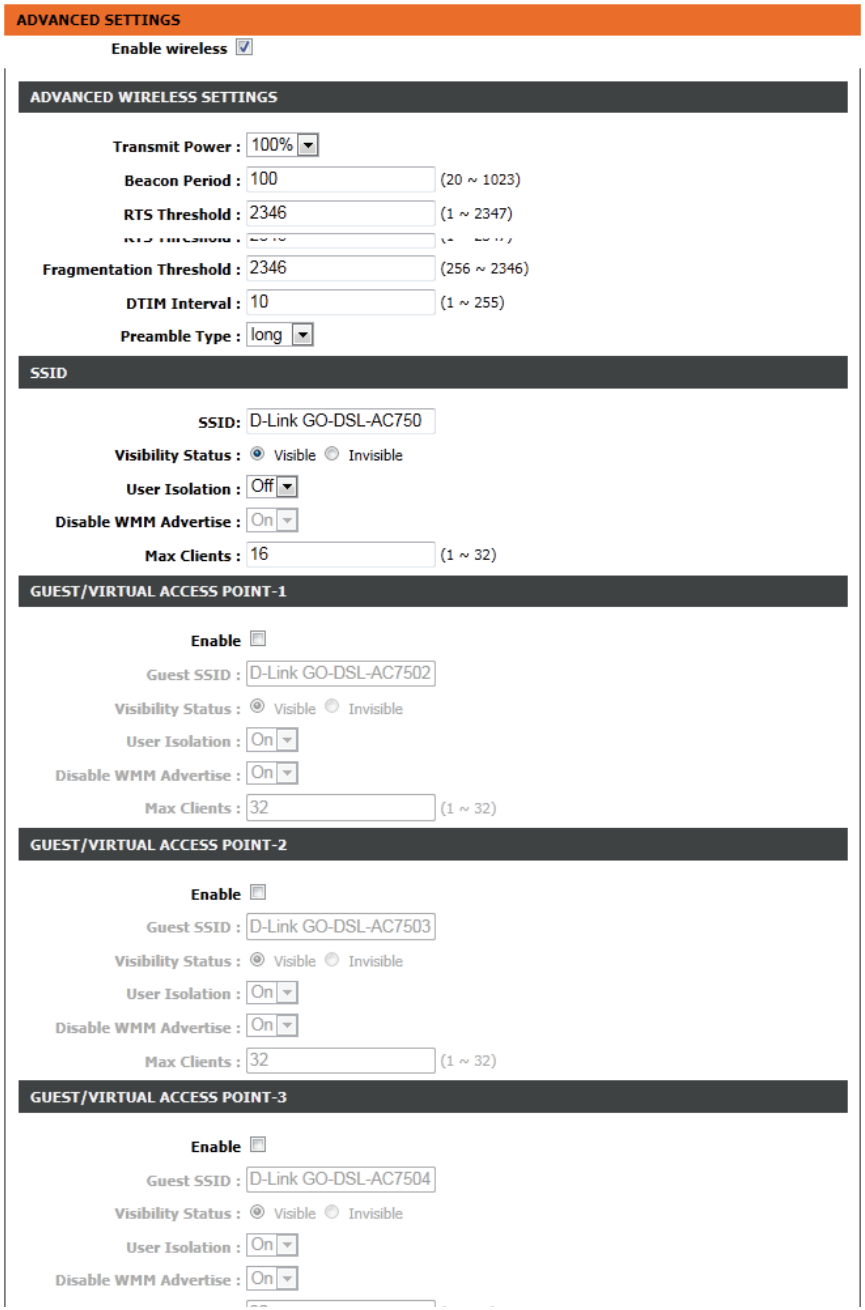
Guest SSID: Specify a name for each guest network.

Visibility Status: Enable the guest wireless network to be Visible or Invisible to wireless clients.

User Isolation: Choose to enable or disable guest wireless user isolation.

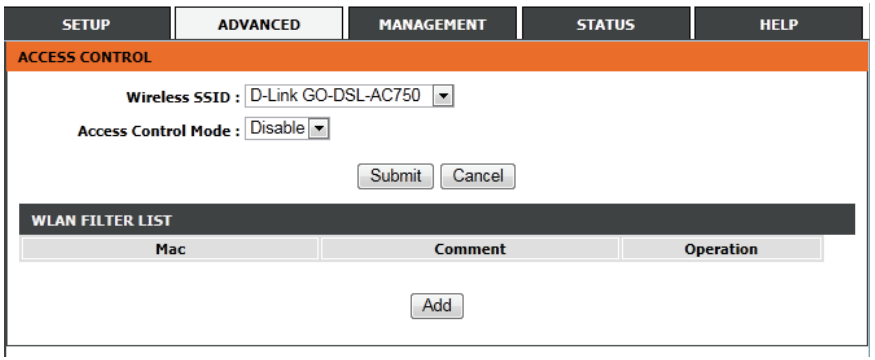
Disable WMM Advertise: Enable or Disable WiFi MultiMedia QoS on the guest network.

Max Clients: Use this option to specify the maximum number of clients on the guest network.


ADVANCED SETTINGS
Enable wireless
ADVANCED WIRELESS SETTINGS
Transmit Power : 100%
Beacon Period : 100 (20 ~ 1023)
RTS Threshold : 2346 (1 ~ 2347)
Fragmentation Threshold : 2346 (256 ~ 2346)
DTIM Interval : 10 (1 ~ 255)
Preamble Type : long
SSID
SSID: D-Link GO-DSL-AC750
Visibility Status : Visible Invisible
User Isolation : Off
Disable WMM Advertise : On
Max Clients : 16 (1 ~ 32)
GUEST/VIRTUAL ACCESS POINT-1
Enable
Guest SSID : D-Link GO-DSL-AC7502
Visibility Status : Visible Invisible
User Isolation : On
Disable WMM Advertise : On
Max Clients : 32 (1 ~ 32)
GUEST/VIRTUAL ACCESS POINT-2
Enable
Guest SSID : D-Link GO-DSL-AC7503
Visibility Status : Visible Invisible
User Isolation : On
Disable WMM Advertise : On
Max Clients : 32 (1 ~ 32)
GUEST/VIRTUAL ACCESS POINT-3
Enable
Guest SSID : D-Link GO-DSL-AC7504
Visibility Status : Visible Invisible
User Isolation : On
Disable WMM Advertise : On

MAC Filtering

The Access Control setup tab enables you to configure filters to control which wireless clients access your network, and which network resources they can access.

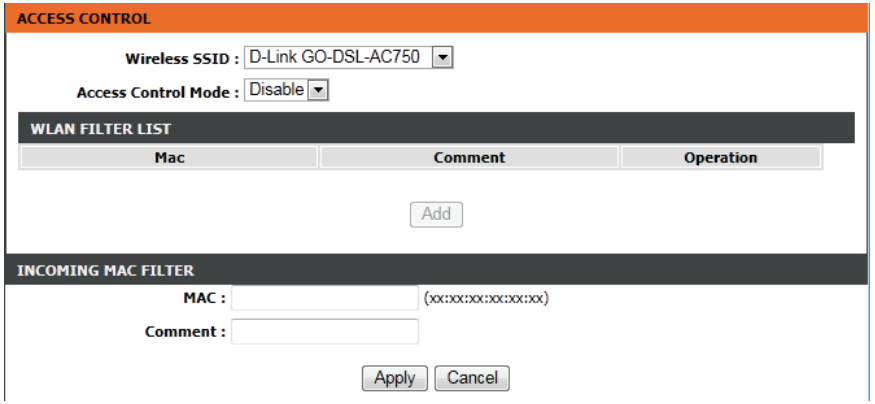


Select **Enable** to enable the Wireless Access Control Mode. In this mode, only listed wireless devices will be allowed to connect to the wireless network.

Click the **Add** button to add an item to the filter list.

Enter the MAC Address of a device you wish to allow access for to the WLAN.

Click the **Apply** button when you are done. This will add the device's MAC Address to the filter list.



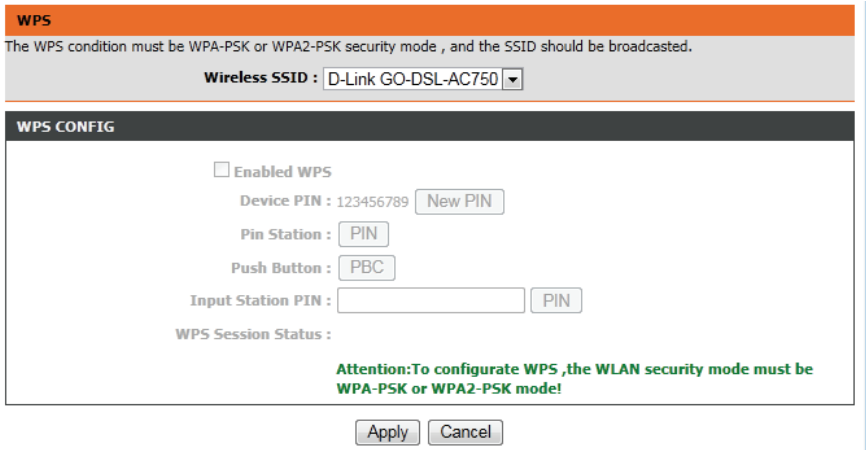
Security Settings

Select the SSID of the virtual network you wish to configure.

Select a wireless security encryption option. You can also choose to not use one by selecting **None**, but this is **not recommended**. For information on wireless security, please refer to "Wireless Security" on page 117.

WPS Settings

This section allows you to configure how the GO-DSL-AC750 uses Wi-Fi Protected Setup (WPS) to create a secure wireless connection.


WPS
The WPS condition must be WPA-PSK or WPA2-PSK security mode , and the SSID should be broadcasted.
Wireless SSID : D-Link GO-DSL-AC750
WPS CONFIG
Enabled WPS
Device PIN : 123456789 New PIN
Pin Station : PIN
Push Button : PBC
Input Station PIN : PIN
WPS Session Status :
Attention:To configurate WPS ,the WLAN security mode must be WPA-PSK or WPA2-PSK mode!
Apply Cancel

Select the SSID of the virtual network you wish to configure.

Enable WPS: Check the box to enable devices to connect to the router using WPS.

Device PIN: Displays the current PIN (Personal Identification Number) for the router's WPS connection. Wireless clients connecting to the router using the PIN method should enter this PIN in order to connect. Click **New PIN** to generate a new PIN.

PIN Station: Click **PIN** to enter a PIN for the new device that you wish to connect.

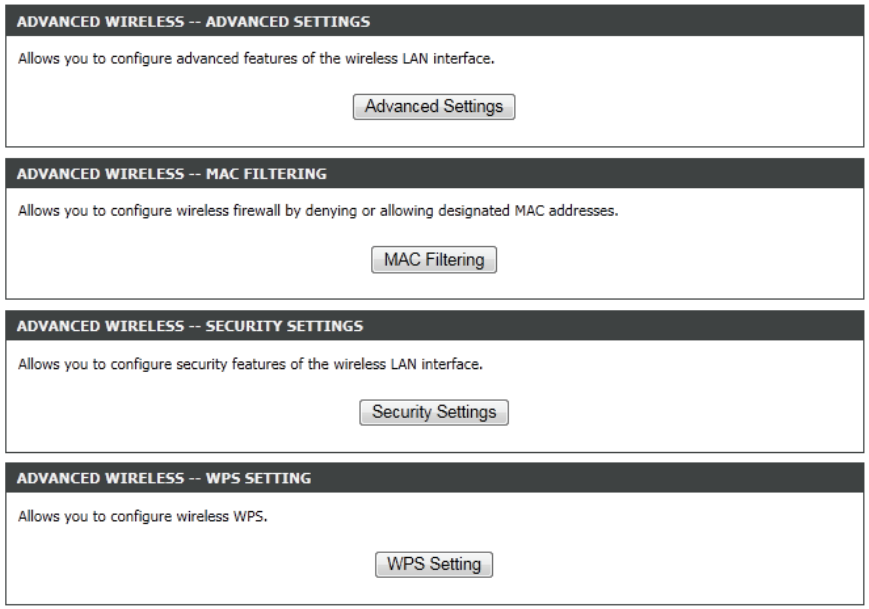
Push Button: Click **PBC** to activate the WPS-PBC (push-button) method. You will then have 120 seconds to press the WPS button on the new device that you wish to connect.

Input Station PIN: Enter the PIN for the station that you wish to connect to. Click **PIN** to connect to the device.

WPS Session Status: Displays the current status of WPS.

5G Advanced Wireless

This section enables you to fine tune the wireless settings on the 5G wireless band.


ADVANCED WIRELESS -- ADVANCED SETTINGS
Allows you to configure advanced features of the wireless LAN interface.
Advanced Settings
ADVANCED WIRELESS -- MAC FILTERING
Allows you to configure wireless firewall by denying or allowing designated MAC addresses.
MAC Filtering
ADVANCED WIRELESS -- SECURITY SETTINGS
Allows you to configure security features of the wireless LAN interface.
Security Settings
ADVANCED WIRELESS -- WPS SETTING
Allows you to configure wireless WPS.
WPS Setting

Advanced Settings

Enable Wireless: Choose to enable or disable the wireless networks.

Transmit Power: Set the transmit power of the antennas in pecentage.

Beacon Period: Beacon Interval range can be set from 20 to 1000.

RTS Threshold: This value should remain at its default setting of 2346. If inconsistent data flow is a problem, only a minor modification should be made.

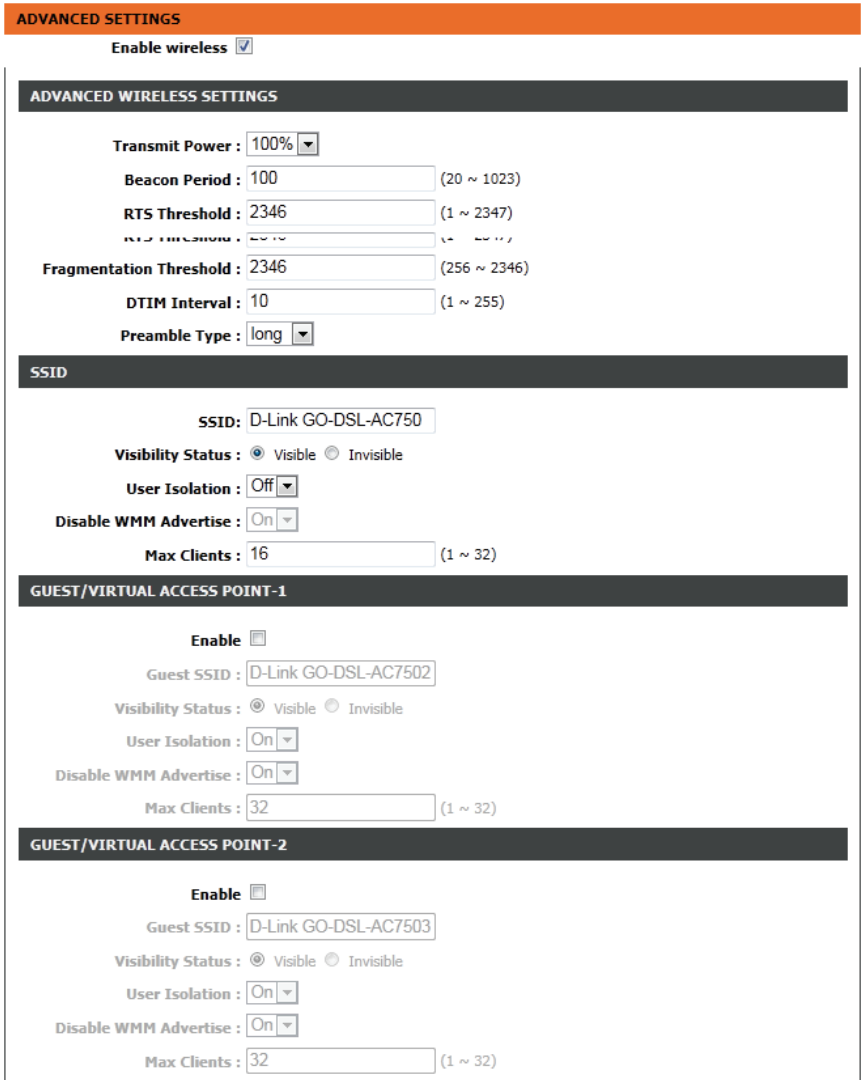
Fragmentation Threshold: The fragmentation threshold, which is specified in bytes, determines whether packets will be fragmented. Packets exceeding the 2346 byte setting will be fragmented before transmission. 2346 is the default setting..

DTIM Interval: DTIM range can be set from 1 to 255. A delivery traffic indication message is a kind of traffic indication message (TIM) which informs the clients of the presence of buffered multicast/broadcast data on the access point.

Preamble Type: Use the dropdown menu to specify whether the Router should use the Short Preamble or Long Preamble type. The preamble type defines the length of the CRC (Cyclic Redundancy Check) block for communication between the Router and roaming wireless adapters

SSID: Enter an SSID for the wireless network.

Visibility Status: Enable the wireless network to be Visible or Invisible to wireless clients. If Invisible, the SSID of the GO-DSL-AC750 will not be seen by site survey utilities, so wireless clients will have to manually enter the SSID of your wireless network in order to connect to it.


ADVANCED SETTINGS
Enable wireless
ADVANCED WIRELESS SETTINGS
Transmit Power : 100%
Beacon Period : 100 (20 ~ 1023)
RTS Threshold : 2346 (1 ~ 2347)
Fragmentation Threshold : 2346 (256 ~ 2346)
DTIM Interval : 10 (1 ~ 255)
Preamble Type : long
SSID
SSID: D-Link GO-DSL-AC750
Visibility Status : Visible Invisible
User Isolation : Off
Disable WMM Advertise : On
Max Clients : 16 (1 ~ 32)
GUEST/VIRTUAL ACCESS POINT-1
Enable
Guest SSID : D-Link GO-DSL-AC7502
Visibility Status : Visible Invisible
User Isolation : On
Disable WMM Advertise : On
Max Clients : 32 (1 ~ 32)
GUEST/VIRTUAL ACCESS POINT-2
Enable
Guest SSID : D-Link GO-DSL-AC7503
Visibility Status : Visible Invisible
User Isolation : On
Disable WMM Advertise : On
Max Clients : 32 (1 ~ 32)

User Isolation: Choose to enable or disable wireless user isolation.

Disable WMM Advertise: Enable or Disable WiFi MultiMedia QoS.

Max Clients: Use this option to specify the maximum number of clients.

Enable Guest Virtual Access Point 1/2/3: Enable or disable a guest network.

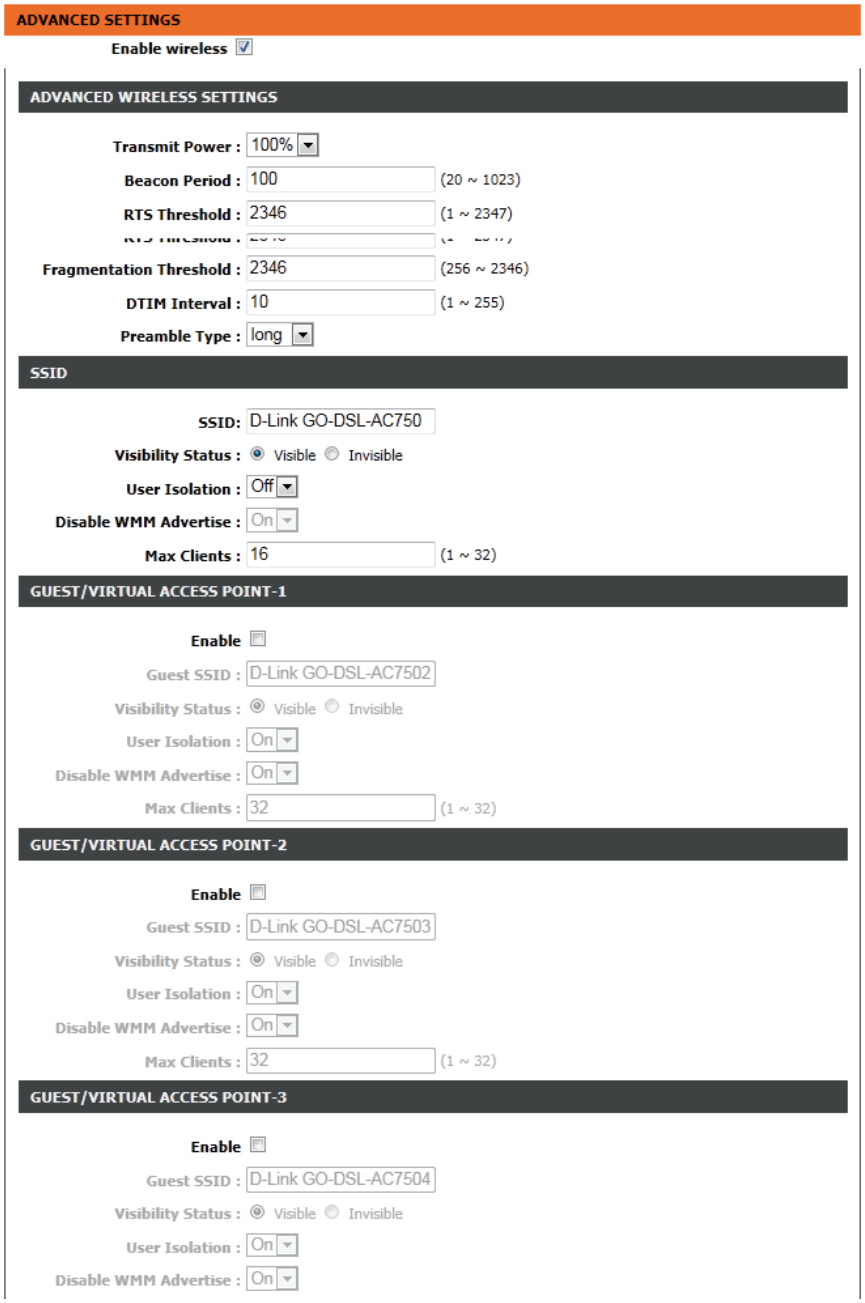
Guest SSID: Specify a name for each guest network.

Visibility Status: Enable the guest wireless network to be Visible or Invisible to wireless clients.

User Isolation: Choose to enable or disable guest wireless user isolation.

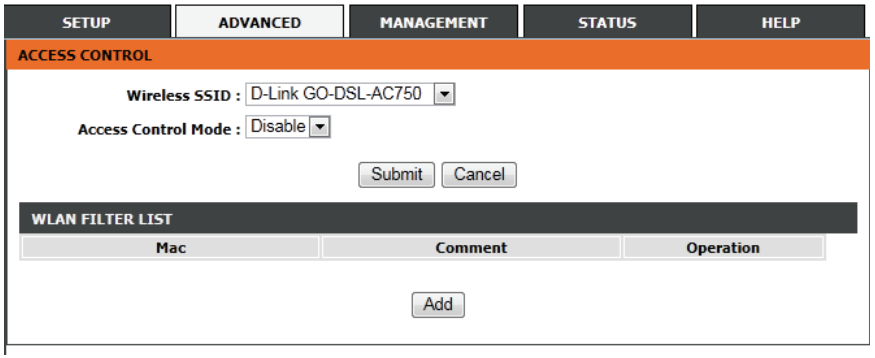
Disable WMM Advertise: Enable or Disable WiFi MultiMedia QoS on the guest network.

Max Clients: Use this option to specify the maximum number of clients on the guest network.


ADVANCED SETTINGS
Enable wireless
ADVANCED WIRELESS SETTINGS
Transmit Power : 100%
Beacon Period : 100 (20 ~ 1023)
RTS Threshold : 2346 (1 ~ 2347)
Fragmentation Threshold : 2346 (256 ~ 2346)
DTIM Interval : 10 (1 ~ 255)
Preamble Type : long
SSID
SSID: D-Link GO-DSL-AC750
Visibility Status : Visible Invisible
User Isolation : Off
Disable WMM Advertise : On
Max Clients : 16 (1 ~ 32)
GUEST/VIRTUAL ACCESS POINT-1
Enable
Guest SSID : D-Link GO-DSL-AC7502
Visibility Status : Visible Invisible
User Isolation : On
Disable WMM Advertise : On
Max Clients : 32 (1 ~ 32)
GUEST/VIRTUAL ACCESS POINT-2
Enable
Guest SSID : D-Link GO-DSL-AC7503
Visibility Status : Visible Invisible
User Isolation : On
Disable WMM Advertise : On
Max Clients : 32 (1 ~ 32)
GUEST/VIRTUAL ACCESS POINT-3
Enable
Guest SSID : D-Link GO-DSL-AC7504
Visibility Status : Visible Invisible
User Isolation : On
Disable WMM Advertise : On

MAC Filtering

The Access Control setup tab enables you to configure filters to control which wireless clients access your network, and which network resources they can access.

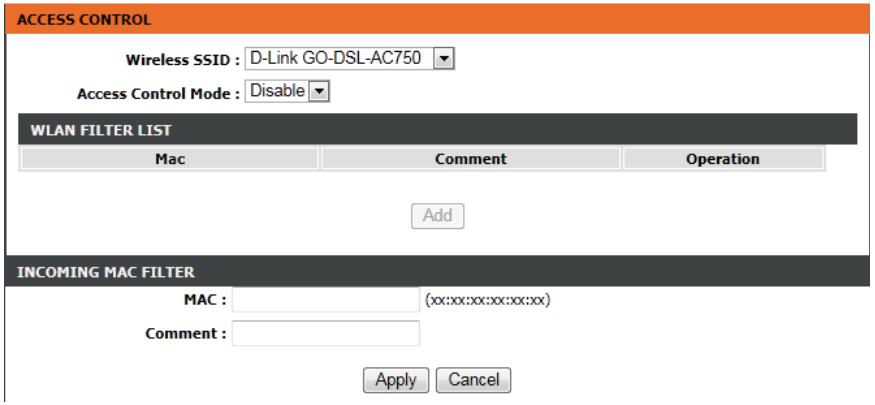


Select **Enable** to enable the Wireless Access Control Mode. In this mode, only listed wireless devices will be allowed to connect to the wireless network.

Click the **Add** button to add an item to the filter list.

Enter the MAC Address of a device you wish to allow access for to the WLAN.

Click the **Apply** button when you are done. This will add the device's MAC Address to the filter list.



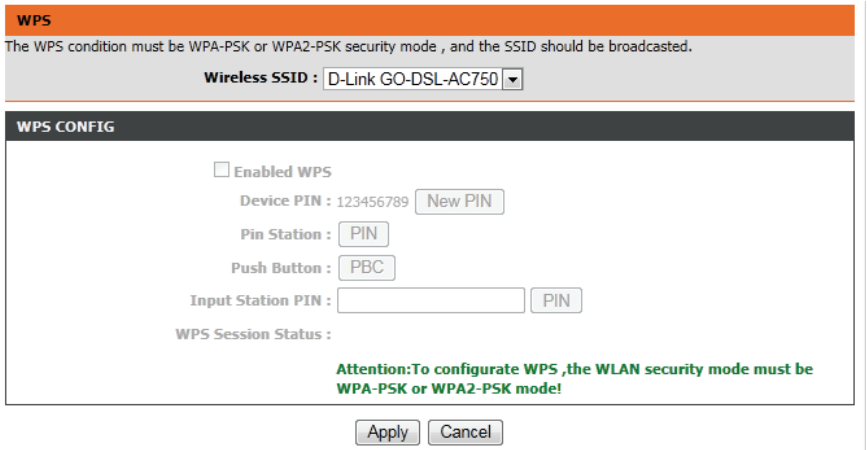
Security Settings

Select the SSID of the virtual network you wish to configure.

Select a wireless security encryption option. You can also choose to not use one by selecting **None**, but this is **not recommended**. For more information on wireless security, please refer to "Wireless Security" on page 117.

WPS Settings

This section allows you to configure how the GO-DSL-AC750 uses Wi-Fi Protected Setup (WPS) to create a secure wireless connection.


WPS
The WPS condition must be WPA-PSK or WPA2-PSK security mode , and the SSID should be broadcasted.
Wireless SSID : D-Link GO-DSL-AC750
WPS CONFIG
Enabled WPS
Device PIN : 123456789 New PIN
Pin Station : PIN
Push Button : PBC
Input Station PIN : PIN
WPS Session Status :
Attention:To configurate WPS ,the WLAN security mode must be WPA-PSK or WPA2-PSK mode!
Apply Cancel

Select the SSID of the virtual network you wish to configure.

Enable WPS: Check the box to enable devices to connect to the router using WPS.

Device PIN: Displays the current PIN (Personal Identification Number) for the router's WPS connection. Wireless clients connecting to the router using the PIN method should enter this PIN in order to connect. Click **New PIN** to generate a new PIN.

PIN Station: Click **PIN** to enter a PIN for the new device that you wish to connect.

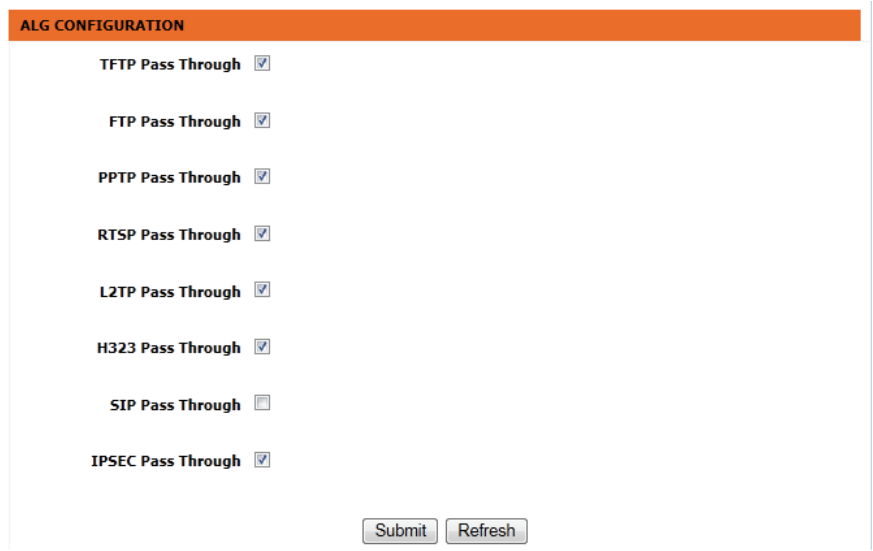
Push Button: Click **PBC** to activate the WPS-PBC (push-button) method. You will then have 120 seconds to press the WPS button on the new device that you wish to connect.

Input Station PIN: Enter the PIN for the station that you wish to connect to. Click **PIN** to connect to the device.

WPS Session Status: Displays the current status of WPS.

ALG

An application-level gateway (ALG) is a security component that augments a firewall or NAT employed in a network. It allows customized NAT filters to support address and port translation for specified application layer protocols.



TFTP Pass Through: Check to enable or disable TFTP pass through functionality.

FTP Pass Through: Check to enable or disable FTP pass through functionality.

PPTP Pass Through: Check to enable or disable PPTP pass through functionality.

RTSP Pass Through: Check to enable or disable RTSP pass through functionality.

L2TP Pass Through: Check to enable or disable L2TP pass through functionality.

H323 Pass Through: Check to enable or disable H323 pass through functionality.

SIP Pass Through: Check to enable or disable SIP pass through functionality.

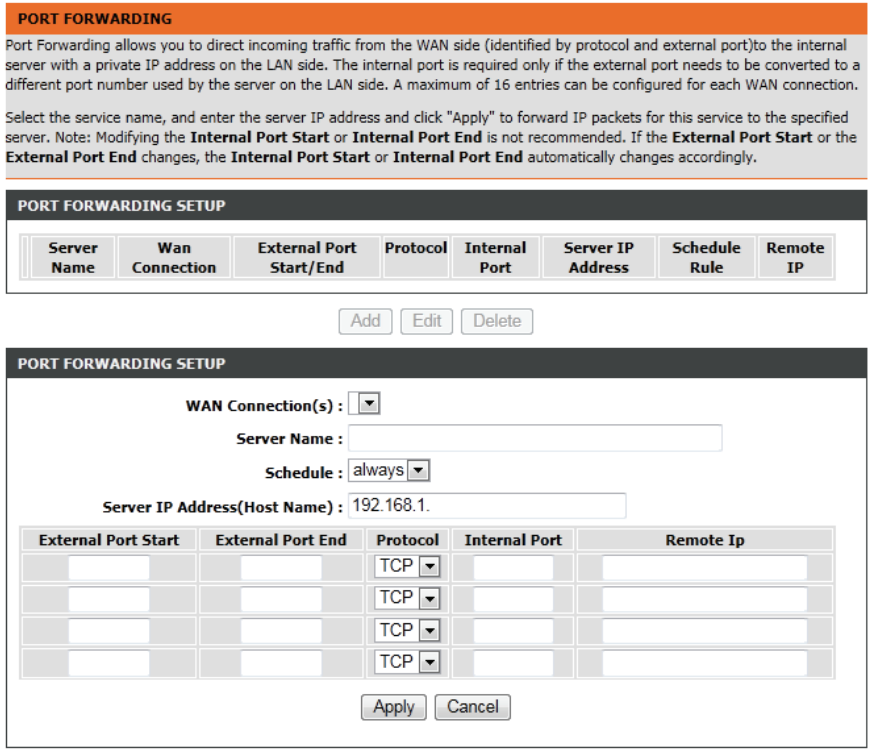
IPSEC Pass Through: Check to enable or disable IPSEC pass through functionality.

Port Forwarding

Port forwarding is a method to direct incoming traffic to a particular server on the LAN. Up to 16 port forwarding entries are supported.

Click **Add**, **Edit**, or **Delete** to reveal the Port forward setup options.

WAN Connection: Specify the WAN connection to use.
Server Name: Enter a name for the server or service.
Schedule: Select a schedule for the port to be forwarded.
Server IP Address: Enter the internal IP address for the traffic to be forwarded to.

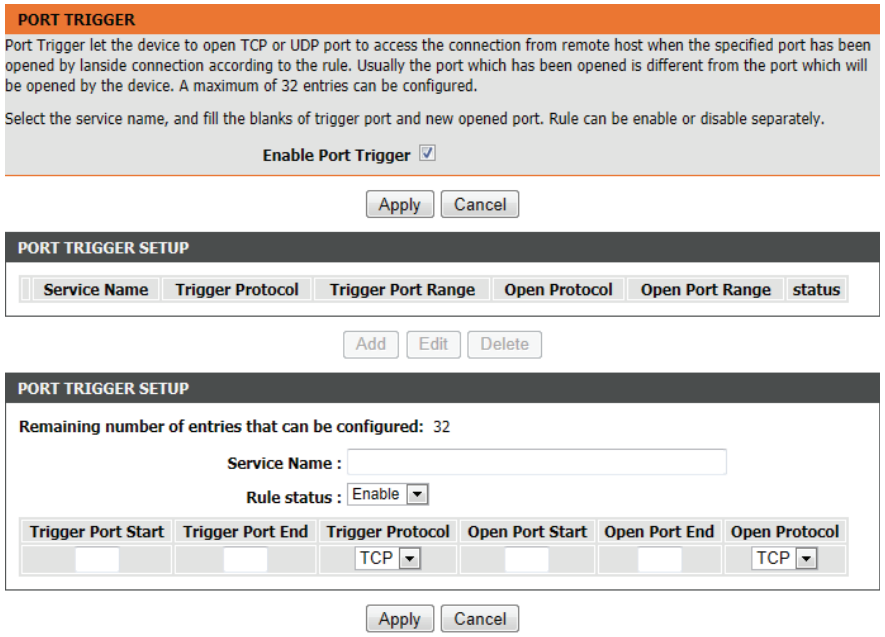

PORT FORWARDING
Port Forwarding allows you to direct incoming traffic from the WAN side (identified by protocol and external port)to the internal server with a private IP address on the LAN side. The internal port is required only if the external port needs to be converted to a different port number used by the server on the LAN side. A maximum of 16 entries can be configured for each WAN connection.
Select the service name, and enter the server IP address and click "Apply" to forward IP packets for this service to the specified server. Note: Modifying the Internal Port Start or Internal Port End is not recommended. If the External Port Start or the External Port End changes, the Internal Port Start or Internal Port End automatically changes accordingly.
PORT FORWARDING SETUP
Server Name
Wan Connection
External Port Start/End
Protocol
Internal Port
Server IP Address
Schedule Rule
Remote IP
Add
Edit
Delete
PORT FORWARDING SETUP
WAN Connection(s) :
Server Name :
Schedule :
always
Server IP Address(Host Name) :
192.168.1.
External Port Start
External Port End
Protocol
Internal Port
Remote Ip
TCP
TCP
TCP
TCP
Apply
Cancel

Port Trigger

Port triggering allows ports to be opened for remote access if triggered by activity by a local computer on specified ports.

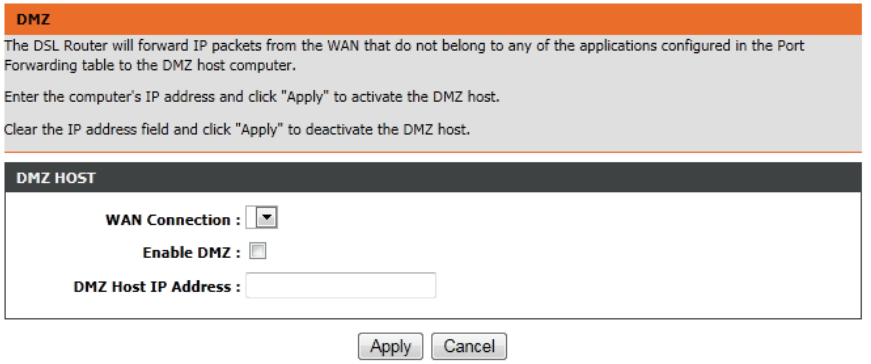
Click **Add**, **Edit**, or **Delete** to reveal the Port Trigger setup options.

Enable Port Trigger: Check this to enable the port trigger feature.
Service Name: Enter a name for the server or service.
Rule Status: Select whether to Enable or Disable this rule.
Trigger Port Start/End: Enter the starting and ending port to monitor to trigger this rule.
Trigger Protocol: Enter the protocol to monitor for to trigger this rule.
Open Port Start/End: Enter the starting and ending port to open when the rule is triggered.
Open Protocol: Enter the protocol to allow through the opened ports.


PORT TRIGGER
Port Trigger let the device to open TCP or UDP port to access the connection from remote host when the specified port has been opened by lanside connection according to the rule. Usually the port which has been opened is different from the port which will be opened by the device. A maximum of 32 entries can be configured.
Select the service name, and fill the blanks of trigger port and new opened port. Rule can be enable or disable separately.
Enable Port Trigger
Apply
Cancel
PORT TRIGGER SETUP
Service Name
Trigger Protocol
Trigger Port Range
Open Protocol
Open Port Range
status
Add
Edit
Delete
PORT TRIGGER SETUP
Remaining number of entries that can be configured: 32
Service Name :
Rule status :
Enable
Trigger Port Start
Trigger Port End
Trigger Protocol
Open Port Start
Open Port End
Open Protocol
TCP
TCP
Apply
Cancel

DMZ

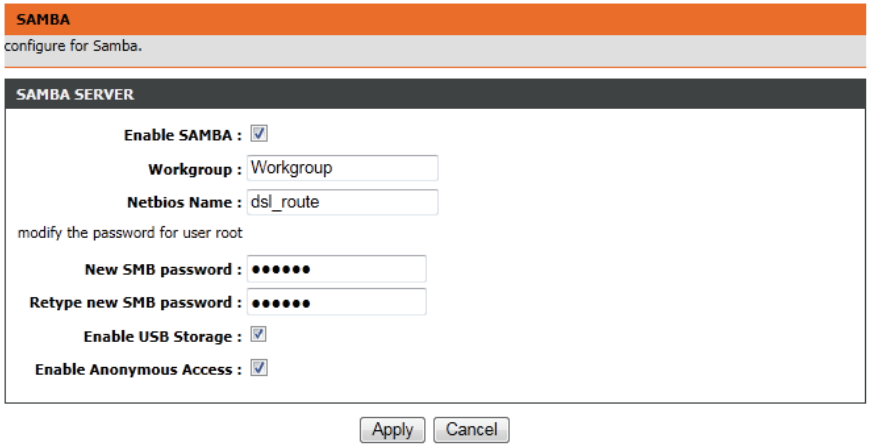
A DMZ or Demilitarized Zone is as a physical or logical subnetwork that contains and exposes external-facing services to a larger and untrusted network, usually the Internet.


DMZ
The DSL Router will forward IP packets from the WAN that do not belong to any of the applications configured in the Port Forwarding table to the DMZ host computer.
Enter the computer's IP address and click "Apply" to activate the DMZ host.
Clear the IP address field and click "Apply" to deactivate the DMZ host.
DMZ HOST
WAN Connection :
Enable DMZ :
DMZ Host IP Address :
Apply
Cancel

WAN Connection: Specify the WAN connection to use.
Enable DMZ: Check to enable or disable DMZ functionality.
DMZ Host IP Address: Enter an IP address to be inlcuded in the DMZ.

SAMBA

Samba allows cross platform file and print sharing between computers. It is an implementation of dozens of services and a dozen protocols.



Enable SAMBA: Check to enable or disable SAMBA functionality.

Workgroup: Enter the name of the workgroup to be mapped.

Netbios Name: Enter a name for Netbios mapping.

New SMB password: Enter a password for the root user.

Retype new SMB password: Re-enter the password for the root user.

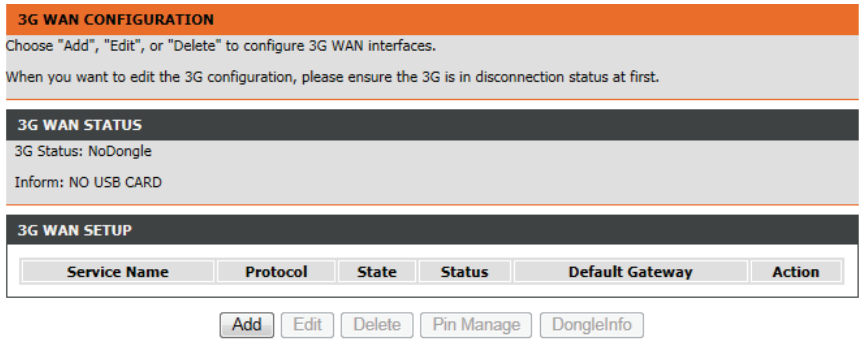
Enable USB Storage: Check to enable or disable SAMBA functionality for USB devices.

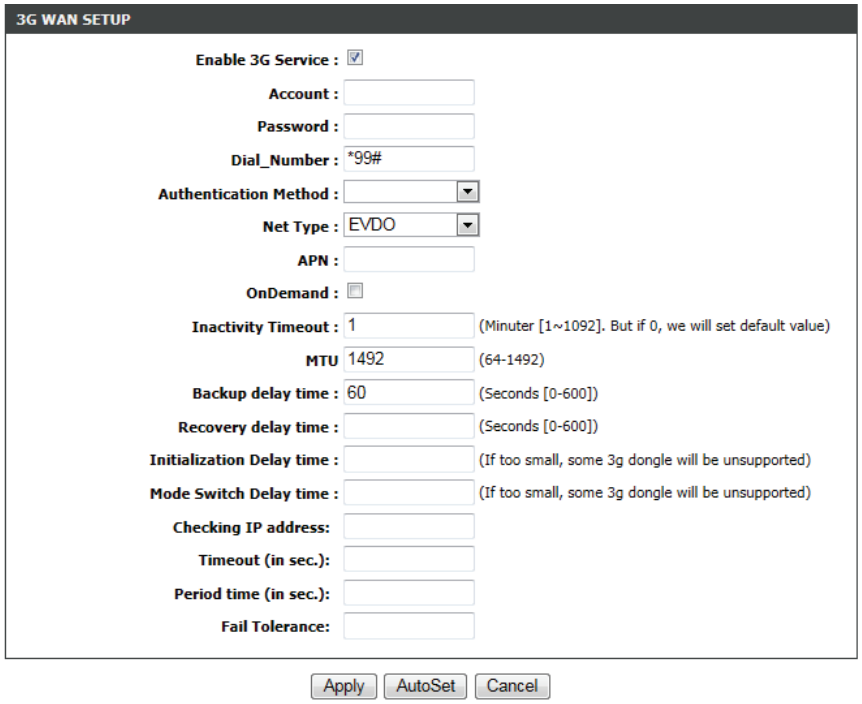
Enable Anonymous Access: Check to enable or disable SAMBA functionality for USB anonymous users.

3G WAN Configuration

This section enables you to configure a 3G Internet connection. Click the **Add** button to reveal the setup options.

Enable 3G Service Check to enable or disable 3G functionality.
Account: Enter your 3G Account username.
Password: Enter your 3G Account password.
Dial Number: Enter the number to be dialed.
Net Type: Select your 3G network access type.
APN: Enter the Access Point Network if there is one.
On Demand: Check to connect to 3G network automatically or manually.
Inactivity Timeout: Enter a period to disconnect an inactive connection.
Backup delay time: The response time allowed for 3G connection before a dial-up is initiated.
Recovery delay time: Specify a period to re-dial.
Initialization Delay time: Specify a period for the 3G connection to initialize.
Mode Switch Delay time: Specify a period to allow for a mode switch.
Backup Mechanism: Select a WAN connection to use if 3G fails.
Checking IP address: Specify an IP Address to test the 3G connection.
Timeout: Specify a period of inactivity after which an established 3G session will be ended. Set to zero or choose Auto in Reconnect Mode to disable this feature.
Period time: Specify a period for DSL or Ethernet uplink to be disconnected.
Fail Tolerance: Specify the number of failures before using the backup connection.



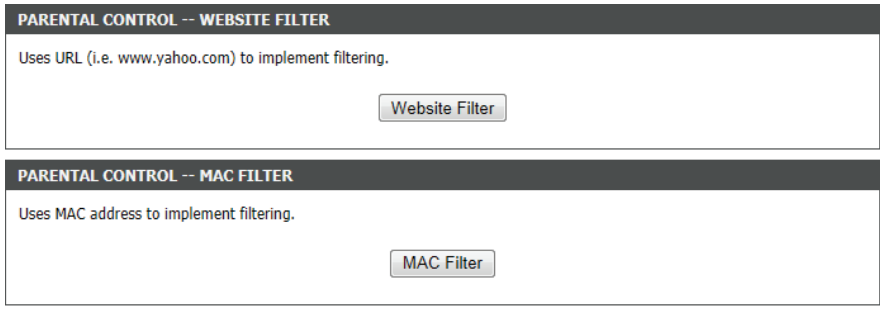

3G WAN SETUP
Enable 3G Service :
Account :
Password :
Dial_Number : *99#
Authentication Method :
Net Type : EVDO
APN :
OnDemand :
Inactivity Timeout : 1 (Minuter [1~1092]. But if 0, we will set default value)
MTU 1492 (64-1492)
Backup delay time : 60 (Seconds [0-600])
Recovery delay time : (Seconds [0-600])
Initialization Delay time : (If too small, some 3g dongle will be unsupported)
Mode Switch Delay time : (If too small, some 3g dongle will be unsupported)
Checking IP address:
Timeout (in sec.):
Period time (in sec.):
Fail Tolerance:
Apply
AutoSet
Cancel

Parental Control

This section enables you to restrict access to the internet.

The **Website Filter** enables you to quickly create a list of websites to limit access to, or to block access to.

The **MAC Filter** enables you to filter access by device MAC addresses.


PARENTAL CONTROL -- WEBSITE FILTER
Uses URL (i.e. www.yahoo.com) to implement filtering.
Website Filter
PARENTAL CONTROL -- MAC FILTER
Uses MAC address to implement filtering.
MAC Filter

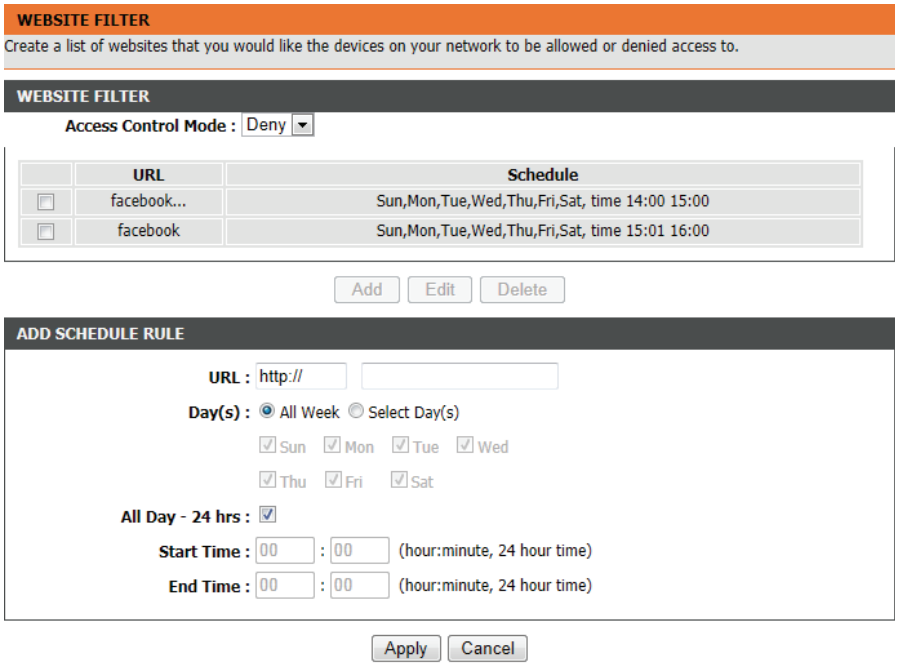
Website Filter

Access Control Mode: Select to **Deny** access to all listed websites, or to **Allow** access to only the listed websites.

Click **Add**/**Edit**/**Delete** to manage your website list.

URL: Enter a website address.

Days/All Day/Start - End Time: Use these options to schedule when you want the website filter to be active for the specified URL.


WEBSITE FILTER
Create a list of websites that you would like the devices on your network to be allowed or denied access to.
WEBSITE FILTER
Access Control Mode : Deny
URL
Schedule
facebook...
Sun,Mon,Tue,Wed,Thu,Fri,Sat, time 14:00 15:00
facebook
Sun,Mon,Tue,Wed,Thu,Fri,Sat, time 15:01 16:00
Add
Edit
Delete
ADD SCHEDULE RULE
URL : http://
Day(s) : All Week Select Day(s)
Sun Mon Tue Wed
Thu Fri Sat
All Day - 24 hrs :
Start Time : 00 : 00 (hour:minute, 24 hour time)
End Time : 00 : 00 (hour:minute, 24 hour time)
Apply
Cancel

MAC Filter

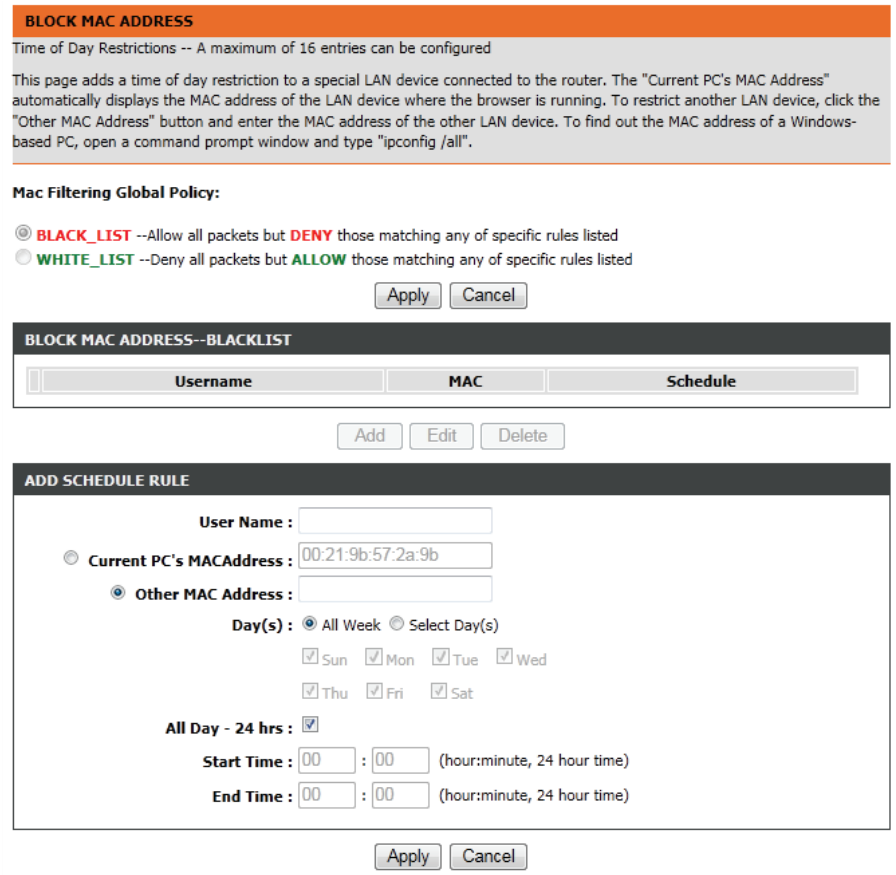
MAC Filtering Global Policy: Choose **BLACK_LIST** or **WHITE_LIST** then click **Add** to reveal the schedule options

User Name: Enter a user name.

Current PC's MAC Address: Enter the users current MAC address.

Other MAC Address: Enter the user's alternate MAC address.

Days/All Day/Start - End Time: Enter or Check the options to create the required access control schedule.


BLOCK MAC ADDRESS
Time of Day Restrictions -- A maximum of 16 entries can be configured
This page adds a time of day restriction to a special LAN device connected to the router. The "Current PC's MAC Address" automatically displays the MAC address of the LAN device where the browser is running. To restrict another LAN device, click the "Other MAC Address" button and enter the MAC address of the other LAN device. To find out the MAC address of a Windows-based PC, open a command prompt window and type "ipconfig /all".
Mac Filtering Global Policy:
BLACK_LIST --Allow all packets but DENY those matching any of specific rules listed
WHITE_LIST --Deny all packets but ALLOW those matching any of specific rules listed
Apply
Cancel
BLOCK MAC ADDRESS--BLACKLIST
Username
MAC
Schedule
Add
Edit
Delete
ADD SCHEDULE RULE
User Name :
Current PC's MACAddress :
00:21:9b:57:2a:9b
Other MAC Address :
Day(s) :
All Week
Select Day(s)
Sun
Mon
Tue
Wed
Thu
Fri
Sat
All Day - 24 hrs :
Start Time :
00
00
(hour:minute, 24 hour time)
End Time :
00
00
(hour:minute, 24 hour time)
Apply
Cancel

Filtering Options

This section enables you to apply advanced IPv4 or IPv6 filtering options .

Click **IPv4 Filtering** to reveal IPv4 configuration options.
Click **IPv6 Filtering** to reveal IPv4 configuration options.

FILTERING OPTIONS -- IP V4 FILTERING
Uses IPv4 address to implement filtering.
IP v4 Filtering
FILTERING OPTIONS -- IP V6 FILTERING
Uses IPv6 address to implement filtering.
IP v6 Filtering

IPv4 Filtering

Enable IP Filter: Check to enable or disable the IPv4 Filter.

Security Level: Select the security level.
Low will set the filter to **Black** in both directions.
Middle will set the filter to **White** in the WAN -> LAN direction and White in the LAN-> WAN direction.
High will set the filter to **White** in both directions.

Filter Model: Select the filter model to adjust and click **Add a Rule** to reveal further options.

Enable: Check to enable or disable the IPv4 model.

Connection: Select the connection to be filtered.

Protocol: Select the appropriate protocol for the connection.

Source IP: Enter the sending IP address to be filtered.

Source Mask: Enter the sending mask to be filtered.

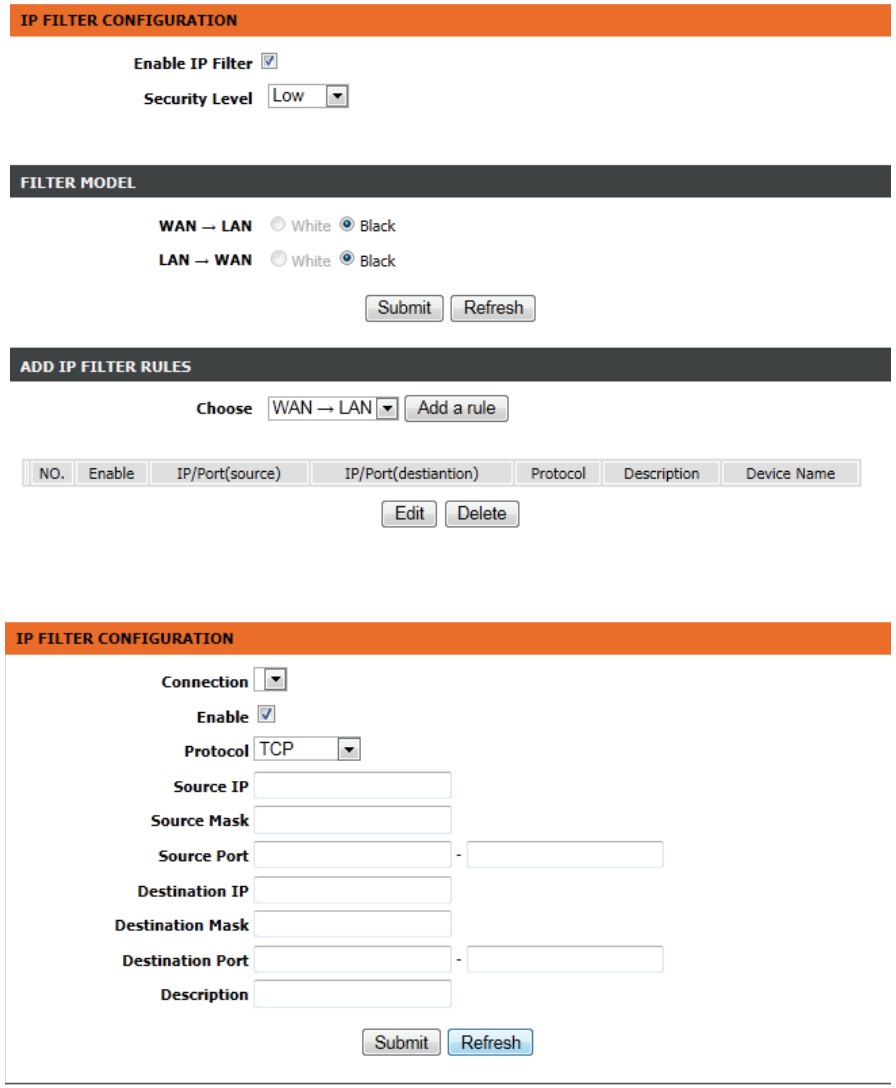
Source Port: Enter the sending port to be filtered.

Destination IP: Enter the destination IP address to be filtered.

Destination Mask: Enter the destination mask to be filtered.

Destination Port: Enter the destination port to be filtered.

Description: Enter a name for the filter rule.



IPv6 Filtering

Enable IP Filter: Check to enable or disable the IPv6 Filter.

Security Level: Select the security level.
Low will set the filter to **Black** in both directions.
Middle will set the filter to **White** in the WAN -> LAN direction and White in the LAN-> WAN direction.
High will set the filter to **White** in both directions.

Filter Model: Select the filter model to adjust and click **Add a Rule** to reveal further options.

Enable: Check to enable or disable the IPv4 model.

Connection: Select the connection to be filtered.

Protocol: Select the appropriate protocol for the connection.

Source IP: Enter the sending IP address to be filtered.

Source Mask: Enter the sending mask to be filtered.

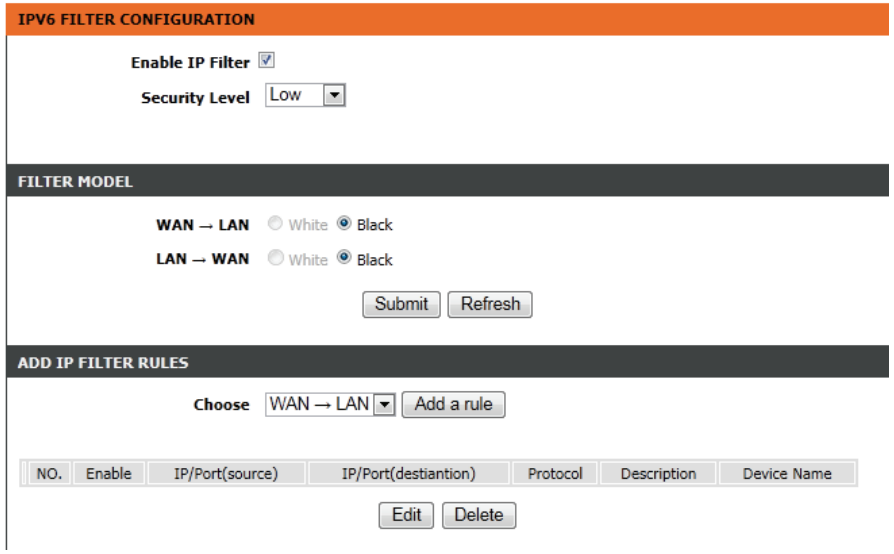
Source Port: Enter the sending port to be filtered.

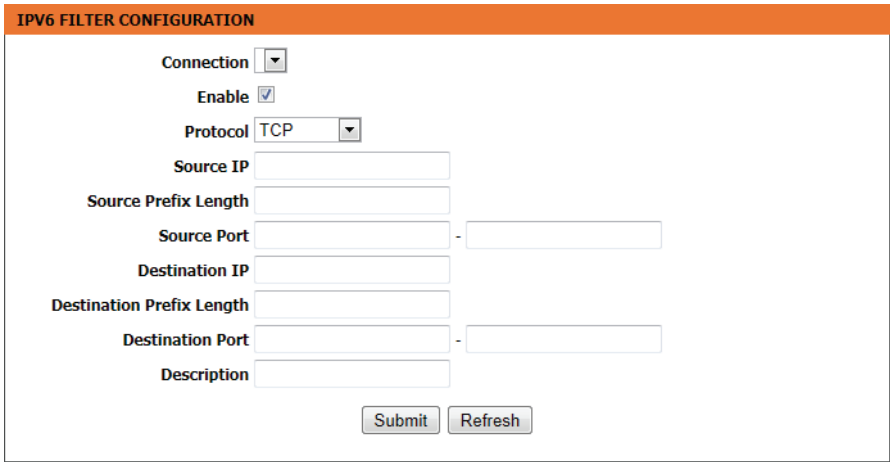
Destination IP: Enter the destination IP address to be filtered.

Destination Mask: Enter the destination mask to be filtered.

Destination Port: Enter the destination port to be filtered.

Description: Enter a name for the filter rule.

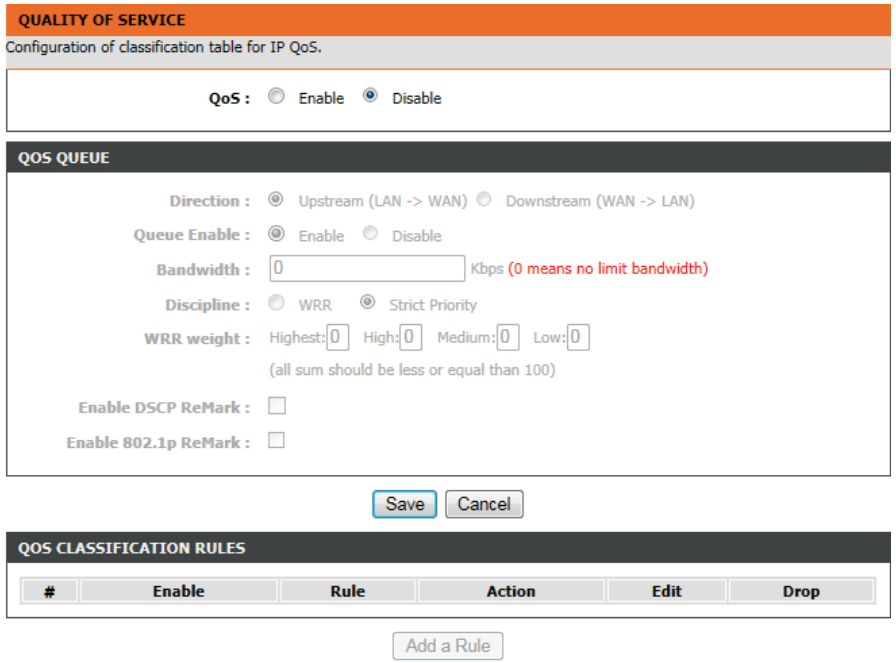




QoS

Quality of Service is a feature that enables you ensure throughput for specific services or devices. QoS can improve your online experience by ensuring that specific traffic is prioritized over other network traffic, such as VoIP, FTP or Web.

QoS: Check to enable or disable QoS.
Direction: Select Upstream or Downstream.
Queue Enable: Check to enable or disable queueing.
Bandwidth: Enter a maximum limit for upstream traffic.
Discipline: Select the QoS discipline type.
WRR Weight: If WRR discipline is selected, define it here.
Enable DSCP ReMark: Check to enable or disable DSCP ReMark.
Enable 802.1p ReMark: Check to enable or disable 802.1p ReMark


QUALITY OF SERVICE
Configuration of classification table for IP QoS.
QoS : Enable Disable
QOS QUEUE
Direction : Upstream (LAN -> WAN) Downstream (WAN -> LAN)
Queue Enable : Enable Disable
Bandwidth : 0 Kbps (0 means no limit bandwidth)
Discipline : WRR Strict Priority
WRR weight : Highest: 0 High: 0 Medium: 0 Low: 0
(all sum should be less or equal than 100)
Enable DSCP ReMark :
Enable 802.1p ReMark :
Save Cancel
QOS CLASSIFICATION RULES
Enable Rule Action Edit Drop
Add a Rule

Click **Add a Rule** to reveal further QoS configuration options.

Add QoS Classification Rules

Classify Type: Check to enable or disable the IPv6 Filter.

Active: Select to enable or disable this rule.

Application: Select the pre-defined application type or choose **Not Matched**.

Physical Ports: Choose the LAN Interface.

Destination MAC address: Enter the destination MAC address for the rule. If data packets include the MAC address, the data packets are placed into the group.

Destination IP address: Enter the destination IP address for the rule. If data packets include the IP address, the data packets are placed into the group.

Destination Subnet Mask: Enter the destination subnet mask for the rule.

Destination Port Range: Enter the destination port range. (eg. UDP/TCP port range)

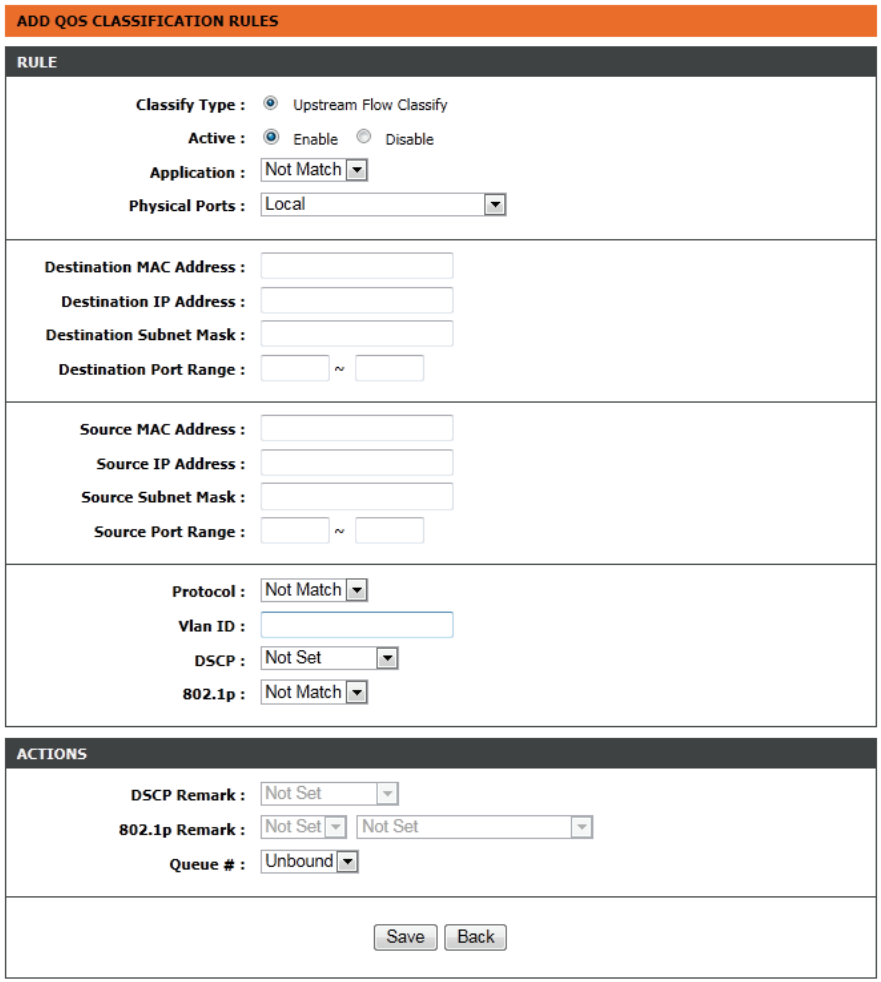
Source MAC address: Enter the source MAC address. If data packets include the MAC address, the data packets are placed into the group.

Source IP address: Enter the source IP address. If data packets include the IP address, the data packets are placed into the group.

Source Subnet Mask: Enter the source subnet mask.

Source Port Range: Enter the source port range. (eg. UDP/TCP port range)

Protocol: Select the pre-defined protocol type or choose **Not Matched**.


ADD QOS CLASSIFICATION RULES
RULE
Classify Type : Upstream Flow Classify
Active : Enable Disable
Application : Not Match
Physical Ports : Local
Destination MAC Address :
Destination IP Address :
Destination Subnet Mask :
Destination Port Range : ~
Source MAC Address :
Source IP Address :
Source Subnet Mask :
Source Port Range : ~
Protocol : Not Match
Vlan ID :
DSCP : Not Set
802.1p : Not Match
ACTIONS
DSCP Remark : Not Set
802.1p Remark : Not Set Not Set
Queue # : Unbound
Save Back

Vlan ID: Select this option to activate or deactivate the 4094 VID on the 4 different queues. VID (VLAN ID) is the identification of the VLAN, which is used by the standard 802.1Q. It has 12 bits and allows the identification of 4096 (2^12) VLANs. Of the 4096 possible VIDs, a VID of 0 is used to identify priority frames and value 4095 (FFF) is reserved. The maximum possible VLAN configurations are 4,094.

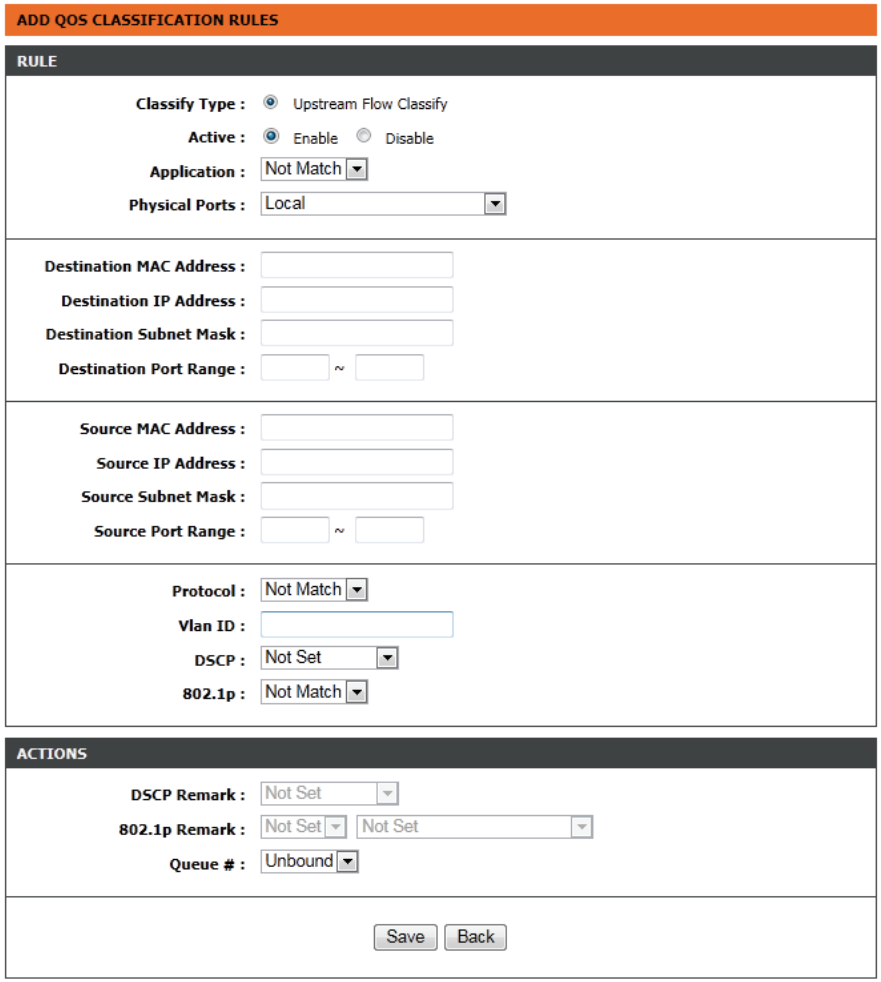
DSCP: Select a matching DSCP type.

802.1p: Select a matching 802.1p VLAN priority

DSCP Remark: The DSCP range can be between 0 to 63.

802.1p Remark: Select this option to Activate/Deactivated the 802.1p. IEEE 802.1p establishes eight levels of priority (0 ~ 7). Although network managers must determine actual mappings, IEEE has made broad recommendations.
Seven is the highest priority which is usually assigned to network-critical traffic such as Routing Information Protocol (RIP) and Open Shortest Path First (OSPF) table updates. Five and six are often for delay-sensitive applications such as interactive video and voice.
Data classes four through one range from controlled-load applications such as streaming multimedia and business-critical traffic - carrying SAP data, for instance - down to "loss eligible" traffic. Zero is used as a best-effort default priority, invoked automatically when no other value has been set

Queue #: Select **Low**, **Medium**, **High** or **Highest**.


ADD QOS CLASSIFICATION RULES
RULE
Classify Type : Upstream Flow Classify
Active : Enable Disable
Application : Not Match
Physical Ports : Local
Destination MAC Address :
Destination IP Address :
Destination Subnet Mask :
Destination Port Range : ~
Source MAC Address :
Source IP Address :
Source Subnet Mask :
Source Port Range : ~
Protocol : Not Match
Vlan ID :
DSCP : Not Set
802.1p : Not Match
ACTIONS
DSCP Remark : Not Set
802.1p Remark : Not Set Not Set
Queue # : Unbound
Save Back

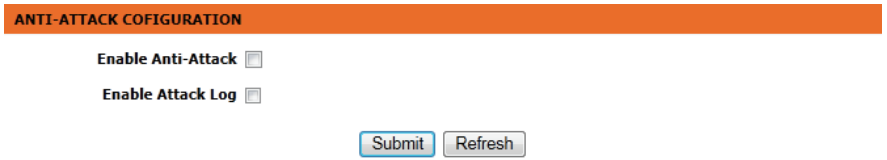
Anti-Attack Settings

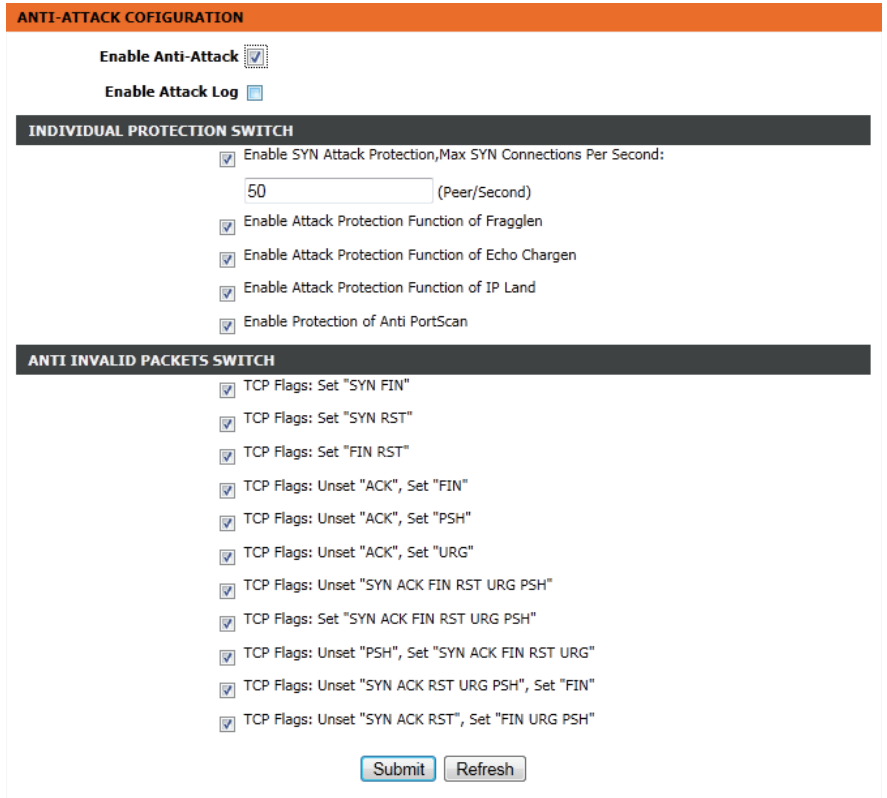
This section enables you to automatically configure your router to detect and protect against several known attack types.

A denial-of-service (DoS) attack is characterized by an explicit attempt by attackers to prevent legitimate users of a service from using that service.

Port scan protection is designed to block attempts to discover vulnerable ports or services that might be exploited in an attack from the WAN.

Check **Enable Anti-Attack** to reveal the Anti- Attack configuration options. Check **Enable Attack Log** to record attack attempts to the log file.



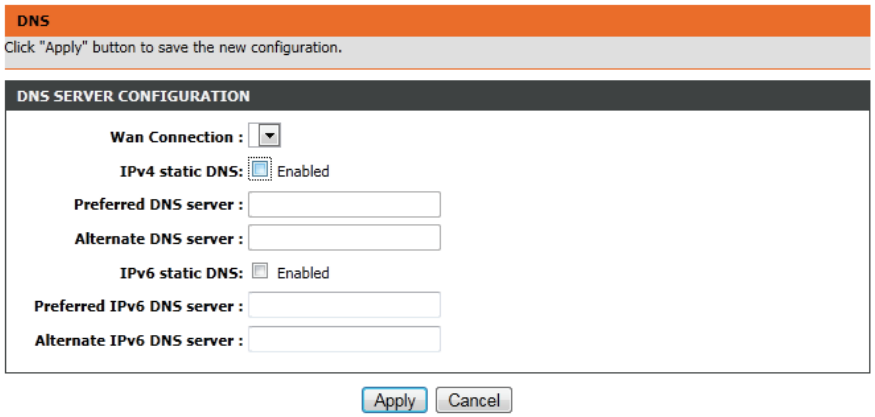

ANTI-ATTACK COFIGURATION
Enable Anti-Attack
Enable Attack Log
INDIVIDUAL PROTECTION SWITCH
Enable SYN Attack Protection,Max SYN Connections Per Second:
50
(Peer/Second)
Enable Attack Protection Function of Fragglen
Enable Attack Protection Function of Echo Chargen
Enable Attack Protection Function of IP Land
Enable Protection of Anti PortScan
ANTI INVALID PACKETS SWITCH
TCP Flags: Set "SYN FIN"
TCP Flags: Set "SYN RST"
TCP Flags: Set "FIN RST"
TCP Flags: Unset "ACK", Set "FIN"
TCP Flags: Unset "ACK", Set "PSH"
TCP Flags: Unset "ACK", Set "URG"
TCP Flags: Unset "SYN ACK FIN RST URG PSH"
TCP Flags: Set "SYN ACK FIN RST URG PSH"
TCP Flags: Unset "PSH", Set "SYN ACK FIN RST URG"
TCP Flags: Unset "SYN ACK RST URG PSH", Set "FIN"
TCP Flags: Unset "SYN ACK RST", Set "FIN URG PSH"
Submit
Refresh

DNS

Domain name system (DNS) is an Internet service that translates domain names into IP addresses. Because domain names are alphabetic, they are easier to remember. The Internet, however, is actually based on IP addresses. Each time you use a domain name, a DNS service must translate the name into the corresponding IP address. For example, the domain name www.example.com might be translated to 198.105.232.4.

The DNS system is, in fact, its own network. If one DNS server does not know how to translate a particular domain name, it asks another one, and so on, until the correct IP address is returned.

If you are using the device for DHCP service on the LAN or using DNS servers on your ISP's network, select **IPv4 static DNS** or **IPv6 static DNS** as appropriate and enter the IP addresses in the available entry fields for the preferred DNS server and the alternate DNS server.

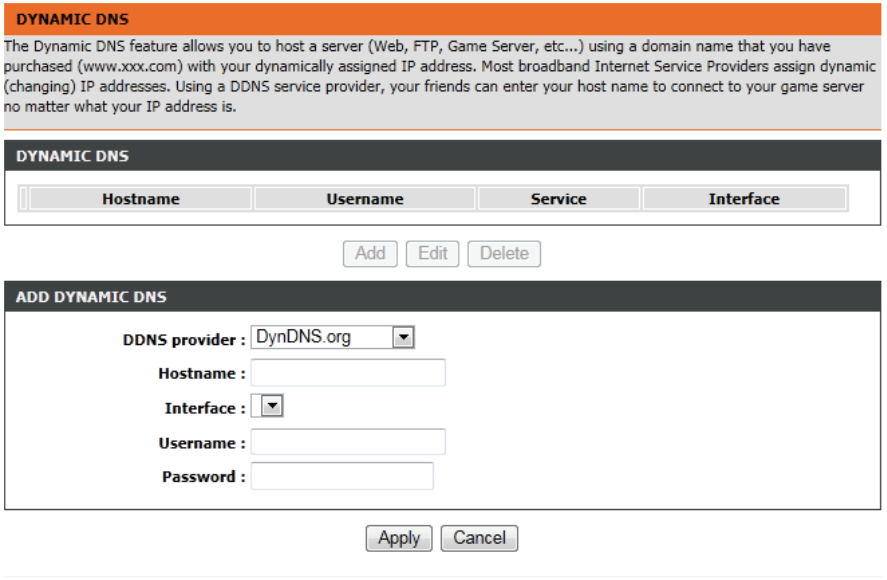


Dynamic DNS

The DDNS (Dynamic Domain Name System) feature allows you to host a server (Web, FTP, Game Server) using a domain name that you have purchased (www.whateveryournameis.com) with your dynamically assigned IP address. Most broadband Internet Service Providers assign dynamic (changing) IP addresses. Using a DDNS service provider, your friends can enter your domain name to connect to your server no matter what your IP address is.

DYNAMIC DNS
The Dynamic DNS feature allows you to host a server (Web, FTP, Game Server, etc...) using a domain name that you have purchased (www.xxx.com) with your dynamically assigned IP address. Most broadband Internet Service Providers assign dynamic (changing) IP addresses. Using a DDNS service provider, your friends can enter your host name to connect to your game server no matter what your IP address is.
DYNAMIC DNS
Hostname
Username
Service
Interface
Add
Edit
Delete

Click **Add** to reveal Dynamic DNS configuration options.


DYNAMIC DNS
The Dynamic DNS feature allows you to host a server (Web, FTP, Game Server, etc...) using a domain name that you have purchased (www.xxx.com) with your dynamically assigned IP address. Most broadband Internet Service Providers assign dynamic (changing) IP addresses. Using a DDNS service provider, your friends can enter your host name to connect to your game server no matter what your IP address is.
DYNAMIC DNS
Hostname
Username
Service
Interface
Add
Edit
Delete
ADD DYNAMIC DNS
DDNS provider :
DynDNS.org
Hostname :
Interface :
Username :
Password :
Apply
Cancel

DDNS provider: Select one of the Dynamic DNS organizations from the menu.

Host Name: Enter the hostname you registered with the Dynamic DNS provider.

Interface: Select the appropriate interface.

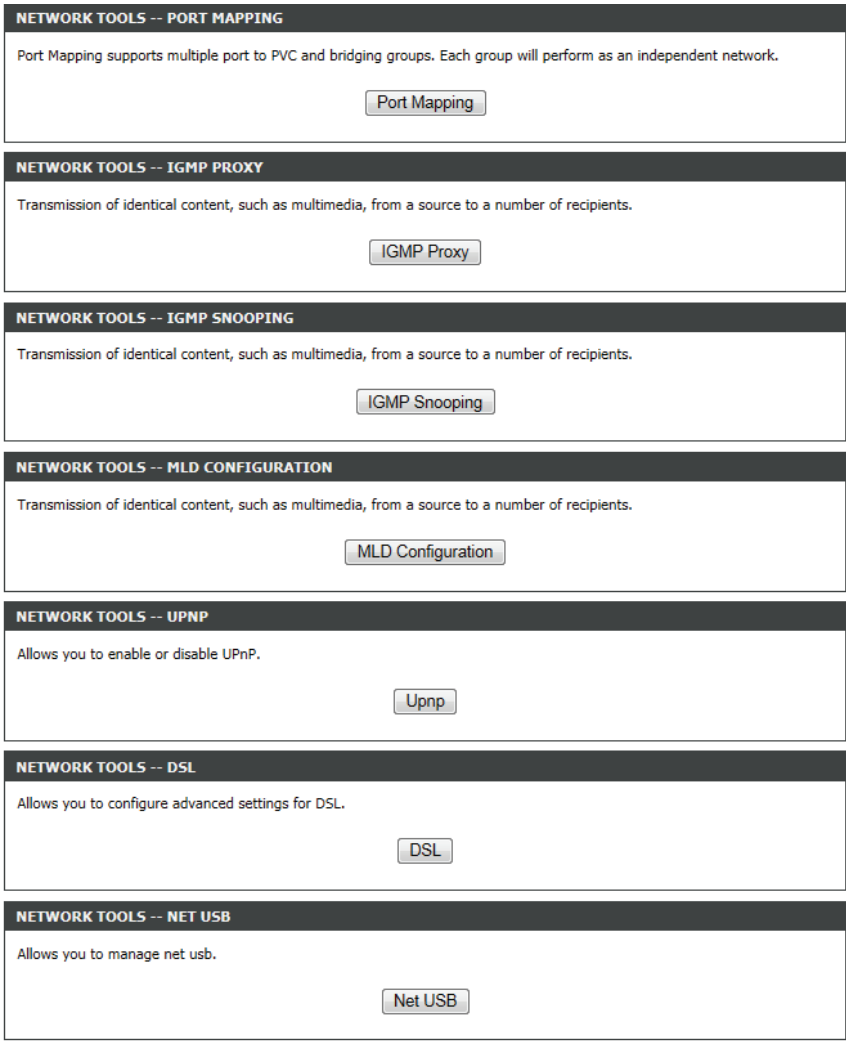
Username: Enter the username for your Dynamic DNS account.

Password: Enter the password for your Dynamic DNS account.

Network Tools

The Network Tools section provides several features which enable a fine degree of network management control.

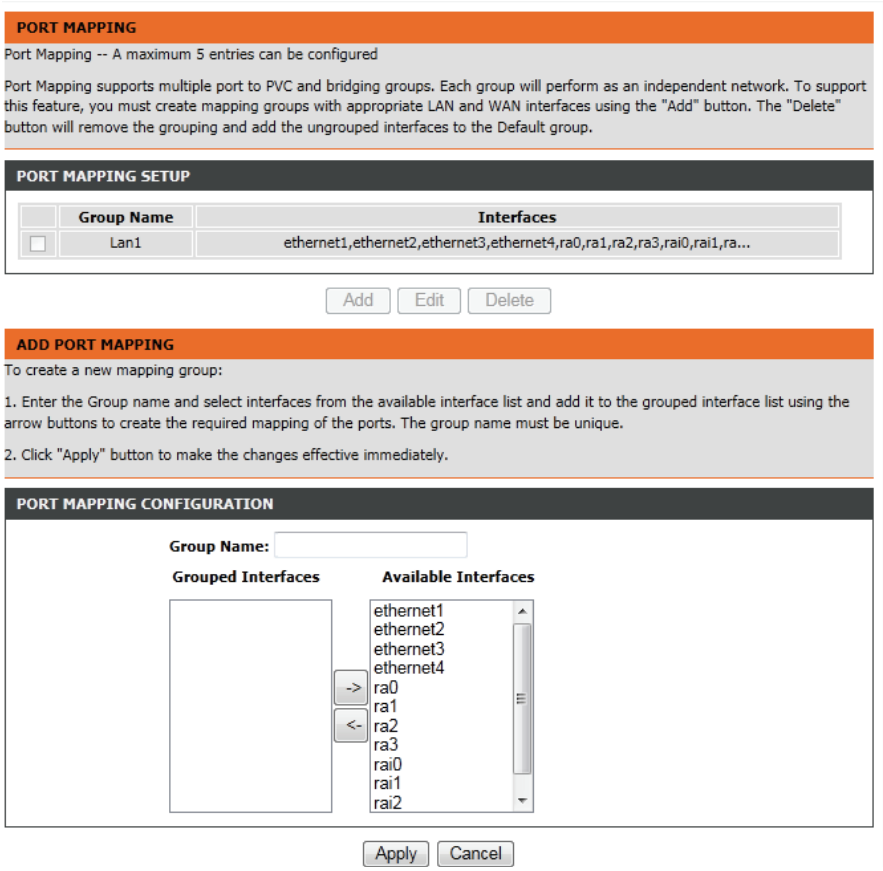
Click the **Port Mapping**, **IGMP Proxy**, **IGMP Snooping**, **MLD Configuration**, **UPnP**, **DSL**, **SNMP**, or **Net USB** button to reveal the associated configuration options.


NETWORK TOOLS -- PORT MAPPING
Port Mapping supports multiple port to PVC and bridging groups. Each group will perform as an independent network.
Port Mapping
NETWORK TOOLS -- IGMP PROXY
Transmission of identical content, such as multimedia, from a source to a number of recipients.
IGMP Proxy
NETWORK TOOLS -- IGMP SNOOPING
Transmission of identical content, such as multimedia, from a source to a number of recipients.
IGMP Snooping
NETWORK TOOLS -- MLD CONFIGURATION
Transmission of identical content, such as multimedia, from a source to a number of recipients.
MLD Configuration
NETWORK TOOLS -- UPNP
Allows you to enable or disable UPnP.
Upnp
NETWORK TOOLS -- DSL
Allows you to configure advanced settings for DSL.
DSL
NETWORK TOOLS -- NET USB
Allows you to manage net usb.
Net USB

Port Mapping

This section enables you to bind the WAN interface and the LAN interface to the same group. This allows remote computers to connect to a specific computer or service within a private local-area network (LAN).

Click **Add** to reveal the Port Mapping configuration options.

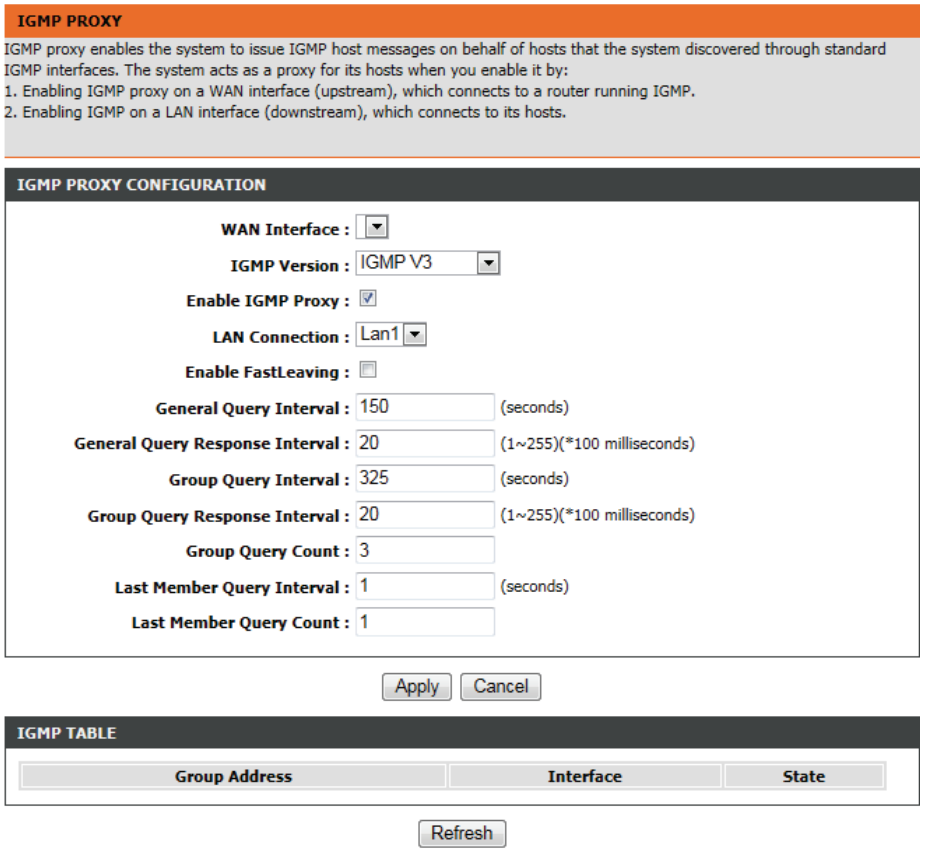

PORT MAPPING
Port Mapping -- A maximum 5 entries can be configured
Port Mapping supports multiple port to PVC and bridging groups. Each group will perform as an independent network. To support this feature, you must create mapping groups with appropriate LAN and WAN interfaces using the "Add" button. The "Delete" button will remove the grouping and add the ungrouped interfaces to the Default group.
PORT MAPPING SETUP
Group Name
Interfaces
Lan1
ethernet1,ethernet2,ethernet3,ethernet4,ra0,ra1,ra2,ra3,rai0,rai1,ra...
Add
Edit
Delete
ADD PORT MAPPING
To create a new mapping group:
1. Enter the Group name and select interfaces from the available interface list and add it to the grouped interface list using the arrow buttons to create the required mapping of the ports. The group name must be unique.
2. Click "Apply" button to make the changes effective immediately.
PORT MAPPING CONFIGURATION
Group Name:
Grouped Interfaces
Available Interfaces
ethernet1
ethernet2
ethernet3
ethernet4
ra0
ra1
ra2
ra3
rai0
rai1
rai2
->
<-
Apply
Cancel

Group Name: Enter a group name.

Group Interfaces: Select from the listed interfaces from the **Available Interface** then click the <- arrow button to add them to the **Grouped Interface** list. This creates the required mapping of the ports. The group name must be unique.

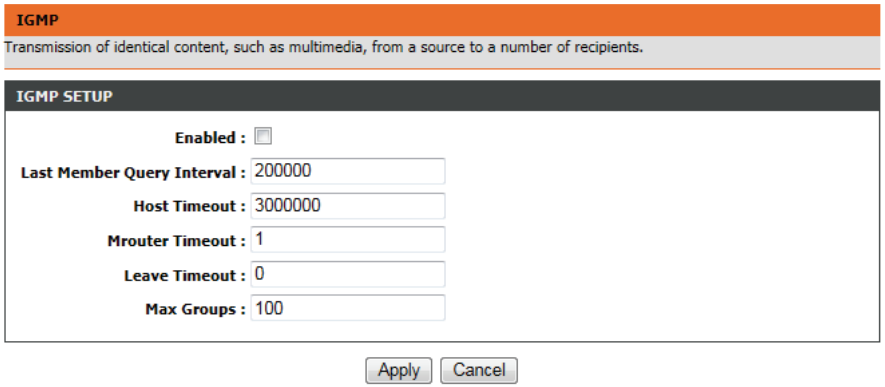
IGMP Proxy

Creating an IGMP proxy enables the system to issue IGMP host messages on behalf of hosts that the system has discovered through standard IGMP interfaces. This allows the system to act as a proxy for its hosts after being enabled.


IGMP PROXY
IGMP proxy enables the system to issue IGMP host messages on behalf of hosts that the system discovered through standard IGMP interfaces. The system acts as a proxy for its hosts when you enable it by:
1. Enabling IGMP proxy on a WAN interface (upstream), which connects to a router running IGMP.
2. Enabling IGMP on a LAN interface (downstream), which connects to its hosts.
IGMP PROXY CONFIGURATION
WAN Interface :
IGMP Version : IGMP V3
Enable IGMP Proxy :
LAN Connection : Lan1
Enable FastLeaving :
General Query Interval : 150 (seconds)
General Query Response Interval : 20 (1~255)(*100 milliseconds)
Group Query Interval : 325 (seconds)
Group Query Response Interval : 20 (1~255)(*100 milliseconds)
Group Query Count : 3
Last Member Query Interval : 1 (seconds)
Last Member Query Count : 1
Apply
Cancel
IGMP TABLE
Group Address
Interface
State
Refresh

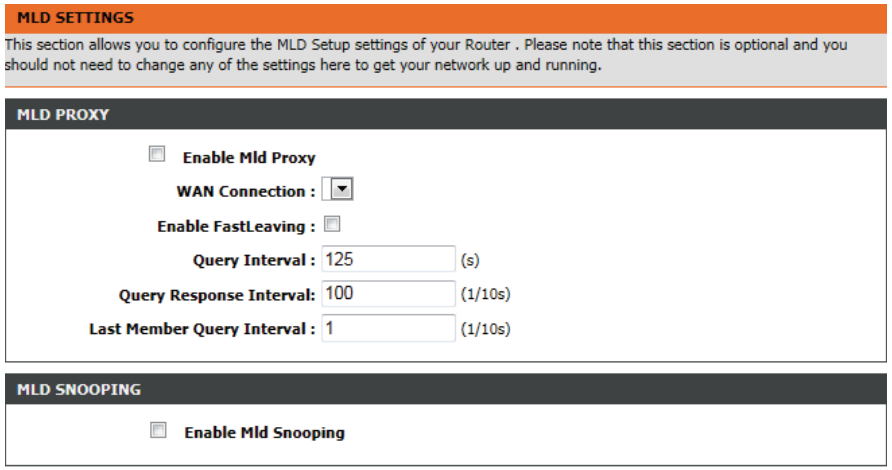
IGMP Snooping

Enabling this option allows the router to listen for internet group management protocol (IGMP) traffic, which can help to detect clients which require multicast streams.


IGMP
Transmission of identical content, such as multimedia, from a source to a number of recipients.
IGMP SETUP
Enabled :
Last Member Query Interval : 200000
Host Timeout : 3000000
Mrouter Timeout : 1
Leave Timeout : 0
Max Groups : 100
Apply
Cancel

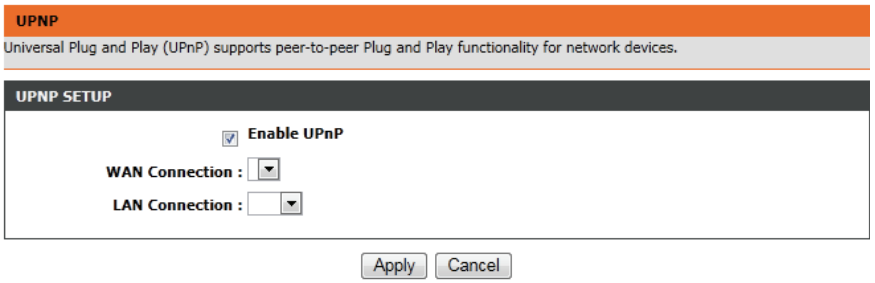
MLD Configuration

Multicast Listener Discovery(MLD) snooping allows the switch to examine MLD packets and make forwarding decisions based on their content.


MLD SETTINGS
This section allows you to configure the MLD Setup settings of your Router . Please note that this section is optional and you should not need to change any of the settings here to get your network up and running.
MLD PROXY
Enable Mld Proxy
WAN Connection :
Enable FastLeaving :
Query Interval : 125 (s)
Query Response Interval: 100 (1/10s)
Last Member Query Interval : 1 (1/10s)
MLD SNOOPING
Enable Mld Snooping

UPnP

This page enables you to configure the UPnP feature.



UPnP (Universal Plug and Play) is a distributed, open networking standard that uses TCP/IP for simple peer-to-peer network connectivity between devices. A UPnP device can dynamically join a network, obtain an IP address, convey its capabilities and learn about other devices on the network. In turn, a device can leave a network smoothly and automatically when it is no longer in use. UPnP broadcasts are only allowed on the LAN.

UPnP is used for popular audio visual software. It allows automatic discovery of your device in the network. If you are concerned about UPnP security, you can disable it. Block ICMP ping should be enabled so that the device does not respond to malicious Internet requests.

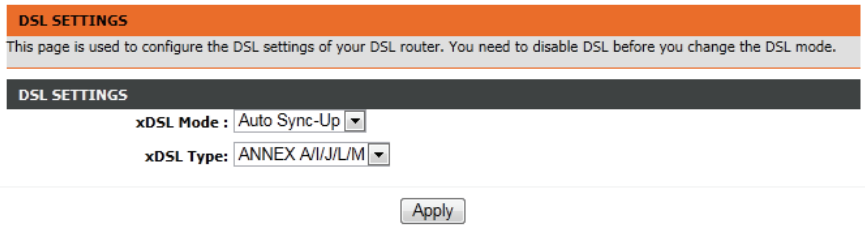
Enable UPnP: Check to enable or disable UPnP.

WAN Connections: Select from the listed interfaces to work with UPnP.

LAN Connections: Select from the listed interfaces to work with UPnP.

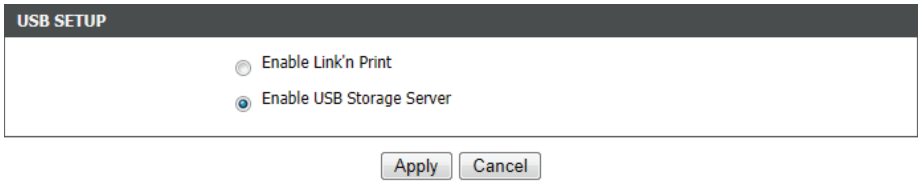
DSL

This page lets you set the xDSL mode and type. It is recommended that you use the default settings.


DSL SETTINGS
This page is used to configure the DSL settings of your DSL router. You need to disable DSL before you change the DSL mode.
DSL SETTINGS
xDSL Mode :
Auto Sync-Up
xDSL Type:
ANNEX A/I/J/L/M
Apply

Net USB

This router comes with a USB 2.0 interface that can connect to a USB printer or storage device such as a USB flash drive or USB hard drive.



Enable Link'n Print: Select this option to use the USB port for connecting a USB printer with D-Link Link'n Print.

D-Link Link'n Print allows you to share your USB printer as a network printer server to all connected local hosts.

Note: Link'n Print Printer Server is a USB printer server which requires users to install a client utility in the computer before the user is able to send a print job to the router.

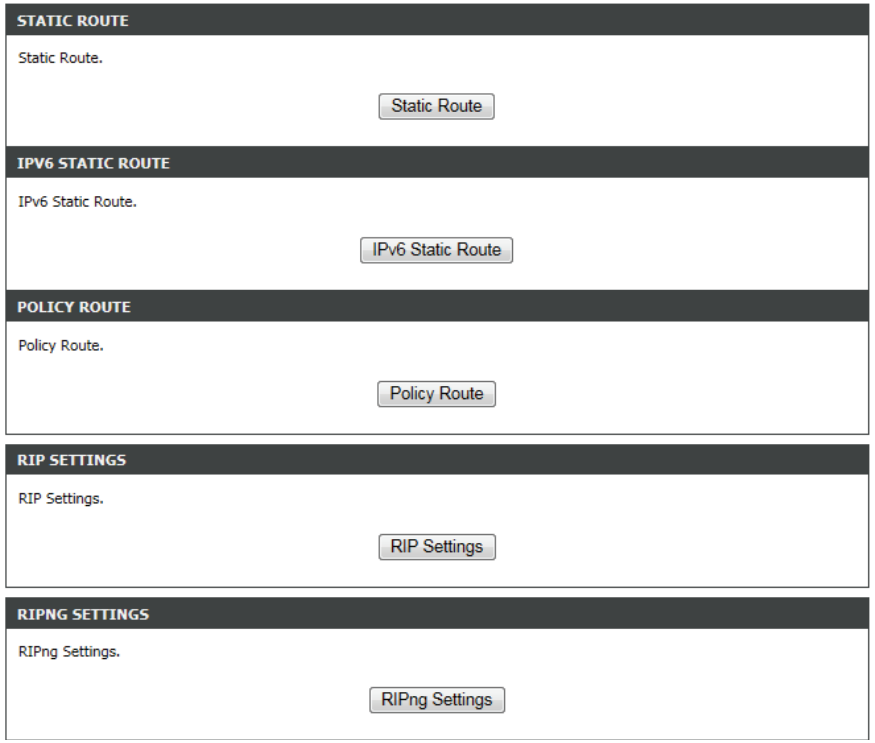
Please refer to "Link'n Print" on page 120 for more information on using this feature.

Enable USB Storage Server: Select this option to use the USB port for connecting a USB storage drive for sharing on your network.

Routing

The Routing sections provides an advanced method of customizing specific routes of data through your network.

Click the **Static Route**, **IPv6 Static Route**, **Policy Route**, **RIP Settings**, or **RIPng Settings** button, to reveal the associated configuration options.



Static Routing

This section allows you to set up static routes for your network.

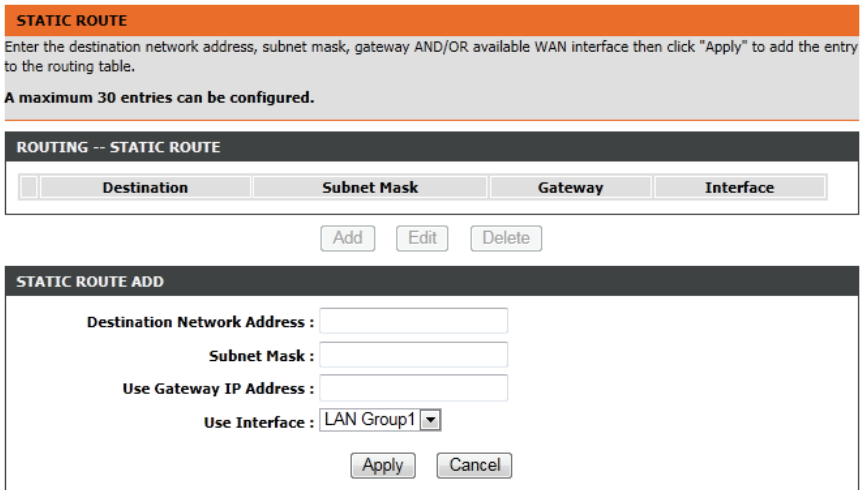
Click the **Add** button to reveal the associated configuration options.

Destination Network Address: Enter the IP address of the destination router.

Subnet Mask: Enter the subnet mask of the destination IP address.

Use Gateway IP Address: Enter the IP address of the gateway router to be used.

Use Interface: Select the interface to be used from the drop-down menu..



IPv6 Static Routing

This section allows you to set up IPv6 static routes for your network.

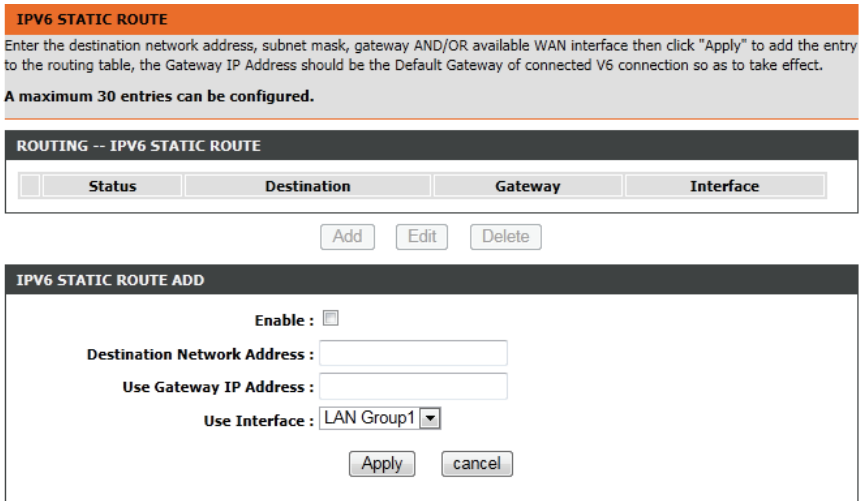
Click the **Add** button to reveal the associated configuration options.

Enable: Check this box to enable the route.

Destination Network Address: Enter the IPv6 address of the destination router.

Use Gateway IP Address: Enter the IPv6 address of the gateway router to be used.

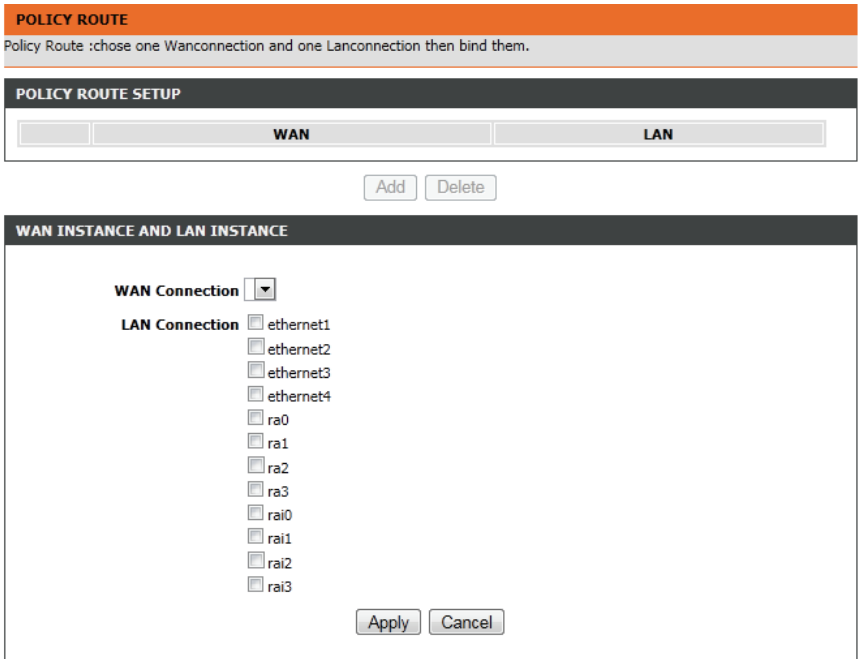
Use Interface: Select the interface to be used from the drop-down menu.


IPV6 STATIC ROUTE
Enter the destination network address, subnet mask, gateway AND/OR available WAN interface then click "Apply" to add the entry to the routing table, the Gateway IP Address should be the Default Gateway of connected V6 connection so as to take effect.
A maximum 30 entries can be configured.
ROUTING -- IPV6 STATIC ROUTE
Status
Destination
Gateway
Interface
Add
Edit
Delete
IPV6 STATIC ROUTE ADD
Enable :
Destination Network Address :
Use Gateway IP Address :
Use Interface :
LAN Group1
Apply
cancel

Policy Route

The Policy Route section provides a method to bind a WAN and at least one LAN connection together.

Click the **Add** button to reveal the associated configuration options.



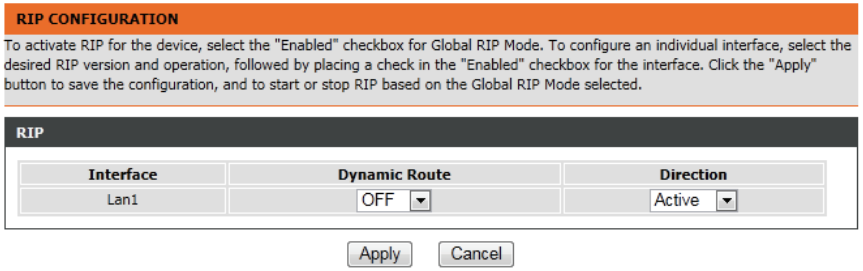
WAN Connection: Select the WAN connection to be used for binding.

LAN Connection: Select at least one LAN connection to be bound.

RIP

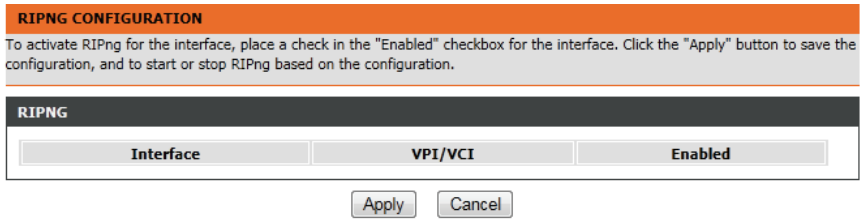
Use this page to select the interfaces on your device that you want to use RIP for, and the version of the protocol to be used.

Dynamic Route: Select from **OFF**, **RIPv1**, **RIPv2**.
Direction: Select either **Active** or **Passive**.


RIP CONFIGURATION
To activate RIP for the device, select the "Enabled" checkbox for Global RIP Mode. To configure an individual interface, select the desired RIP version and operation, followed by placing a check in the "Enabled" checkbox for the interface. Click the "Apply" button to save the configuration, and to start or stop RIP based on the Global RIP Mode selected.
RIP
Interface
Dynamic Route
Direction
Lan1
OFF
Active
Apply
Cancel

RIPng

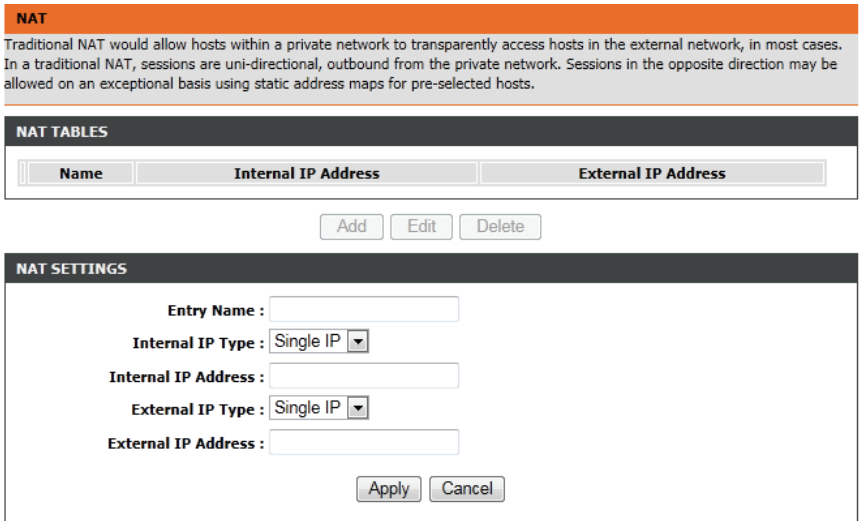
Use this page to enable or disable RIPng for the available interfaces.


RIPNG CONFIGURATION
To activate RIPng for the interface, place a check in the "Enabled" checkbox for the interface. Click the "Apply" button to save the configuration, and to start or stop RIPng based on the configuration.
RIPNG
Interface
VPI/VCI
Enabled
Apply
Cancel

NAT

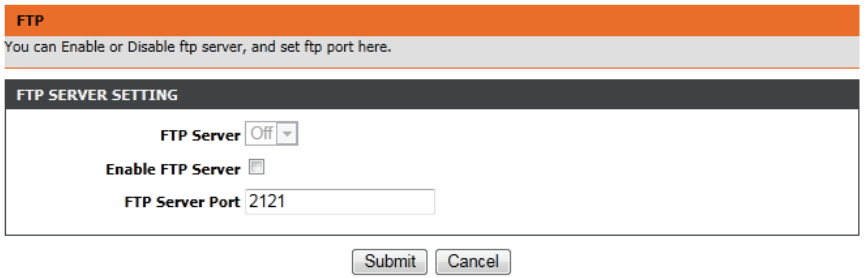
This screen lets you set up NAT for your router to link external IP address with internal IP addresses.

Entry Name: Enter a name for the address to be mapped.
Internal IP Type: Select either **Single IP** or **IP Range**.
Internal IP Address: Enter the IP or the IP Range
External IP Type: Select either **Single IP** or **IP Range**.
External IP Address: Enter the IP or the IP Range


NAT
Traditional NAT would allow hosts within a private network to transparently access hosts in the external network, in most cases. In a traditional NAT, sessions are uni-directional, outbound from the private network. Sessions in the opposite direction may be allowed on an exceptional basis using static address maps for pre-selected hosts.
NAT TABLES
Name
Internal IP Address
External IP Address
Add
Edit
Delete
NAT SETTINGS
Entry Name :
Internal IP Type :
Single IP
Internal IP Address :
External IP Type :
Single IP
External IP Address :
Apply
Cancel

FTPD Setting

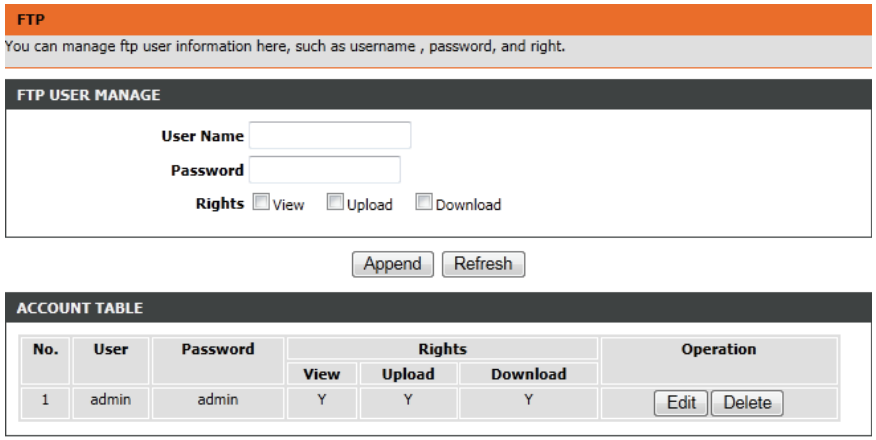
On this page, you can enable or disable the FTP daemon and set the FTP port.



FTP Server: This item displays the FTP server's status.
Enable FTP Server: Select to enable or disable the FTP server.
FTP Server Port: Enter a port for the FTP server.

FTPD Account

On this page, you can add, remove or edit FTP user accounts.


FTP
You can manage ftp user information here, such as username , password, and right.
FTP USER MANAGE
User Name
Password
Rights View Upload Download
Append Refresh
ACCOUNT TABLE
No. User Password Rights Operation
View Upload Download
1 admin admin Y Y Y Edit Delete

User Name: Enter a user name to use for the account.

Password: Enter a password to use for the account.

Rights: Assign **View**, **Upload**, **Download** rights as appropriate for the account.

Append: Append a new account to the Account Table using the User Name, Password, and Rights entered.

Refresh: Refresh an existing account in the Account Table.

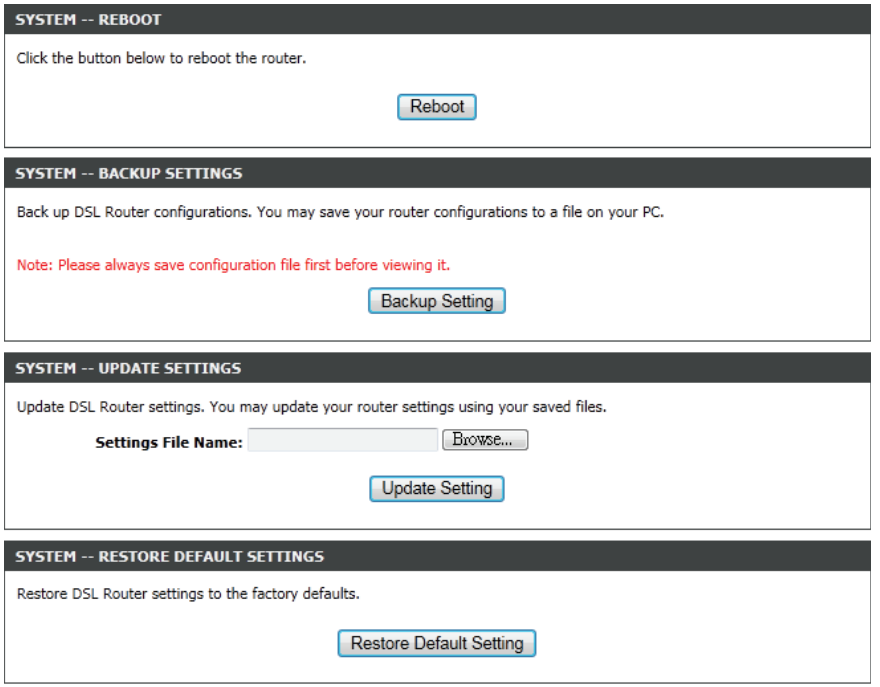
Edit: Edit this account's information. Click the **Modify** button after making your changes to save them.

Delete: Delete this account.

Management

System Management

The System Management sections provides a number of options to manage the Go-DSL-AC750. This section allows you to manage the router's configuration settings, reboot the router, and restore the router to the factory default settings. Restoring the unit to the factory default settings will erase all settings, including any rules that you've created.


SYSTEM -- REBOOT
Click the button below to reboot the router.
Reboot
SYSTEM -- BACKUP SETTINGS
Back up DSL Router configurations. You may save your router configurations to a file on your PC.
Note: Please always save configuration file first before viewing it.
Backup Setting
SYSTEM -- UPDATE SETTINGS
Update DSL Router settings. You may update your router settings using your saved files.
Settings File Name:
Browse...
Update Setting
SYSTEM -- RESTORE DEFAULT SETTINGS
Restore DSL Router settings to the factory defaults.
Restore Default Setting

Reboot: Click **Reboot** to immediately restart the router.

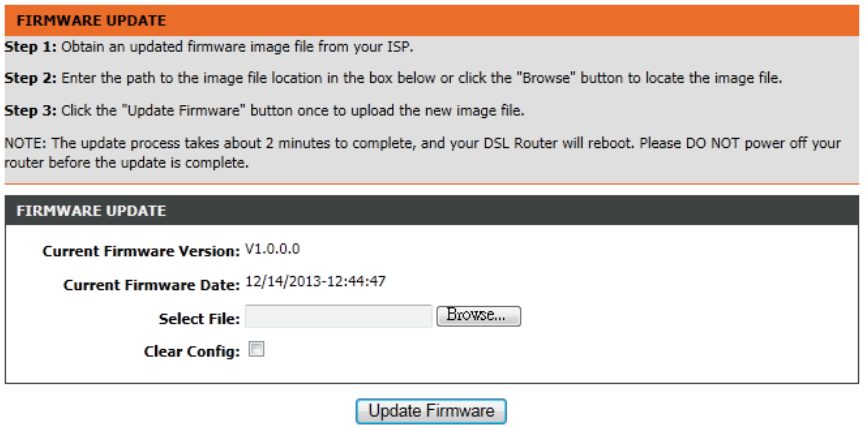
Backup Setting: Use this option to save the current router configuration settings to a file on the hard disk of the computer you are using. First, Click **Backup Setting**. A file dialog will appear, allowing you to select a location and file name for the settings.

Update Setting: Use this option to load previously saved router configuration settings. First, use the **Browse** option to find a previously saved file of configuration settings. Then, click the **Update** button to transfer those settings to the router.

Restore Default Setting: Click **Restore Default Setting** to restore all configuration settings back to the settings that were in effect at the time the router was shipped from the factory. Any settings that have not been saved will be lost, including any rules that you have created.

Firmware Update

You can upgrade the firmware of the access point here. Make sure the firmware you want to use is on the local hard drive of the computer. Click on **Browse** to locate the firmware file to be used for the update. Please check the D-Link support website for firmware updates at **http://support.dlink.com**. You can download firmware upgrades to your hard drive from this site.


FIRMWARE UPDATE
Step 1: Obtain an updated firmware image file from your ISP.
Step 2: Enter the path to the image file location in the box below or click the "Browse" button to locate the image file.
Step 3: Click the "Update Firmware" button once to upload the new image file.
NOTE: The update process takes about 2 minutes to complete, and your DSL Router will reboot. Please DO NOT power off your router before the update is complete.
FIRMWARE UPDATE
Current Firmware Version: V1.0.0.0
Current Firmware Date: 12/14/2013-12:44:47
Select File:
Browse...
Clear Config:
Update Firmware

Current Firmware Version: This fields displays information about the current firmware.

Current Firmware Date: This fields displays the date of the current firmware.

Select File: Click **Browse** to locate the firmware file required.

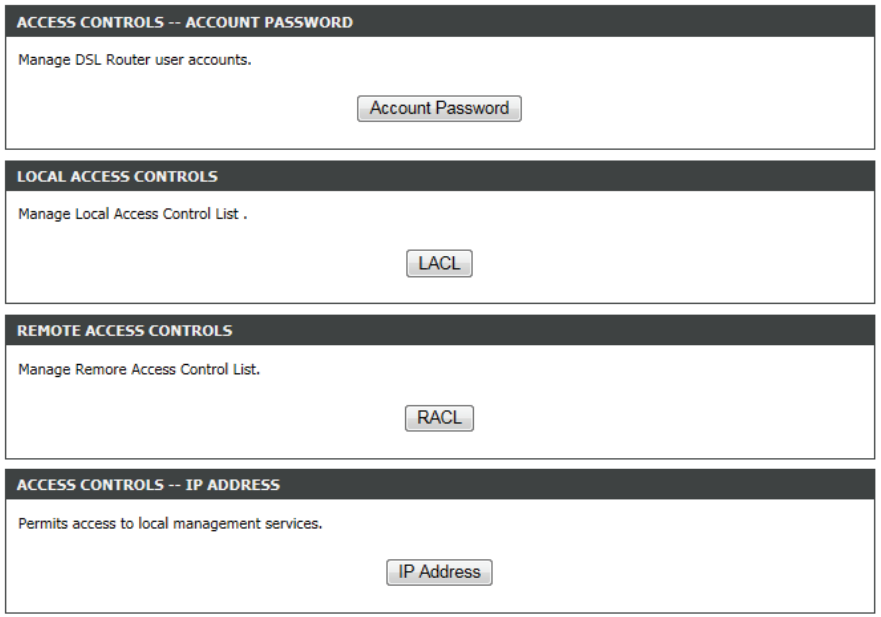
Clear Config: Check **Clear Config** to reset all current configurations before the firmware is installed.

Update Firmware: Click **Update Firmware** to upload and install the selected firmware.

Access Controls

Here, you can manage access to your router.

Click the **Account Password**, **LACL**, **RACL**, or **IP Address** buttons to reveal the associated configuration options.



Account Password

The Account Password section enables you to manage users' passwords.

You should change the default admin password to secure your network.

Ensure that you remember the new password or write it down and keep it in a safe and separate location for future reference. If you forget the password, you will need to reset the device to the factory default settings and all configuration settings of the device will be lost.

Username: Select the username that you want to modify.

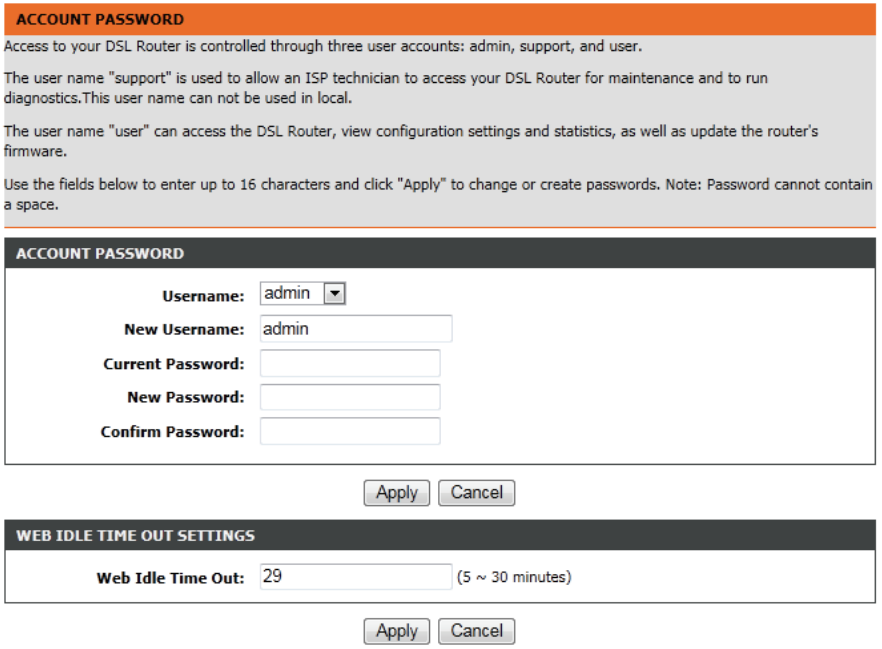
New Username: If you are adding a new user account, enter the username in this field.

Current Password: Enter the current password (existing users only).

New Password: Enter the new password.

Confirm Password: Re-enter the new password.

Web Idle Time Out: Set a period of time to automatically log the user out if the session is inactive for the specified amount of time.

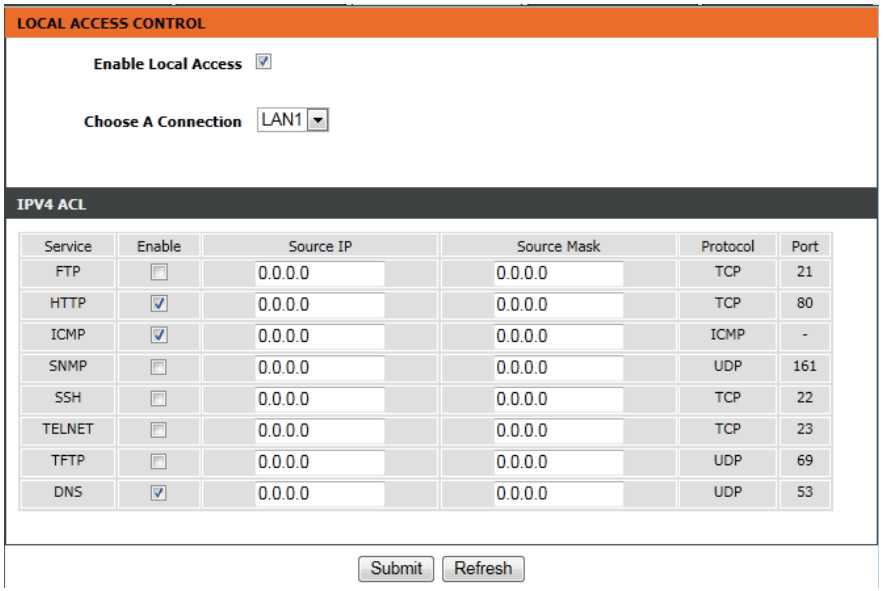

ACCOUNT PASSWORD
Access to your DSL Router is controlled through three user accounts: admin, support, and user.
The user name "support" is used to allow an ISP technician to access your DSL Router for maintenance and to run diagnostics.This user name can not be used in local.
The user name "user" can access the DSL Router, view configuration settings and statistics, as well as update the router's firmware.
Use the fields below to enter up to 16 characters and click "Apply" to change or create passwords. Note: Password cannot contain a space.
ACCOUNT PASSWORD
Username: admin
New Username: admin
Current Password:
New Password:
Confirm Password:
Apply Cancel
WEB IDLE TIME OUT SETTINGS
Web Idle Time Out: 29 (5 ~ 30 minutes)
Apply Cancel

Local Access Control

The Local Access Control section enables you to specify which services can be accessed by a remote host.

Enable Local Access: Check to enable or disable remote access to the following services.

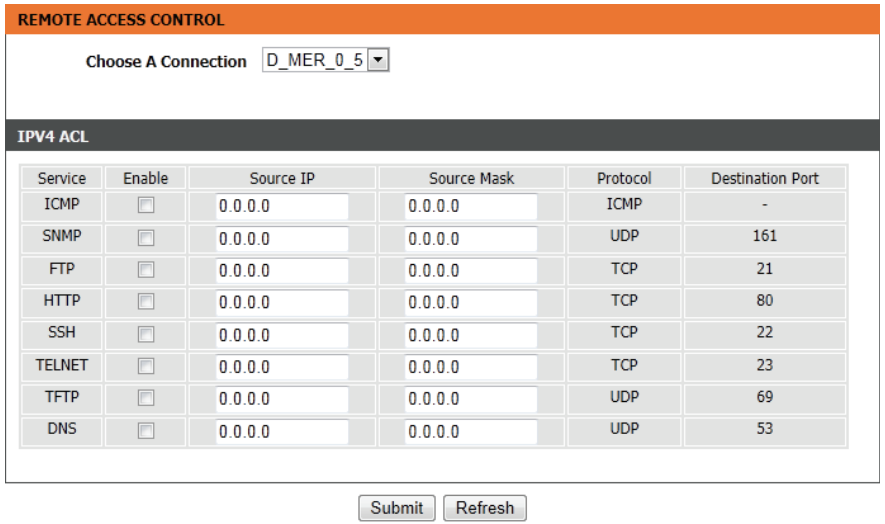
Choose a connection: Select a connection interface from the available options in the dropdown menu.



Remote Access Control

The Remote Access connection section enables you to allow or disallow WAN management access.

Choose a connection: Select a connection from the dropdown menu on which to enable remote access.

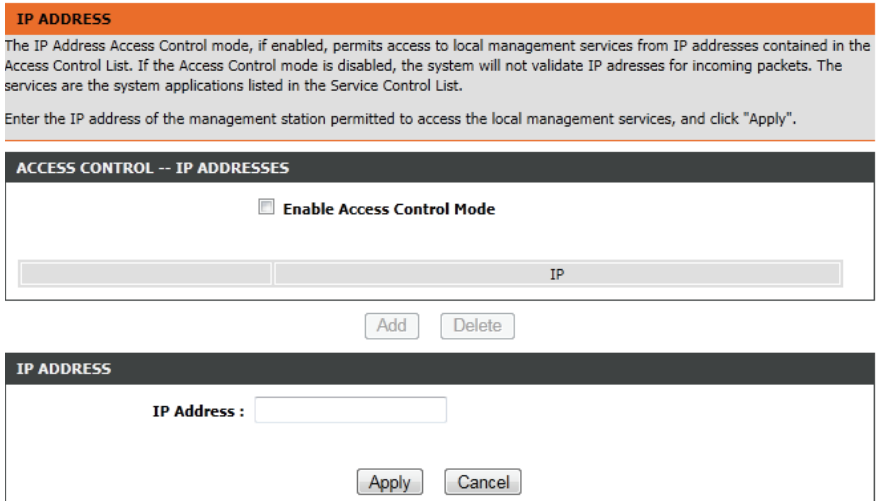


IP Address

On this page, you can configure the IP address for the access control list (ACL). If ACL is enabled, only devices with the specified IP addresses can access the device.

Check **Enable Access Control Mode** to enable the ACL, then click Add, to reveal further options for adding an IP address to the ACL.

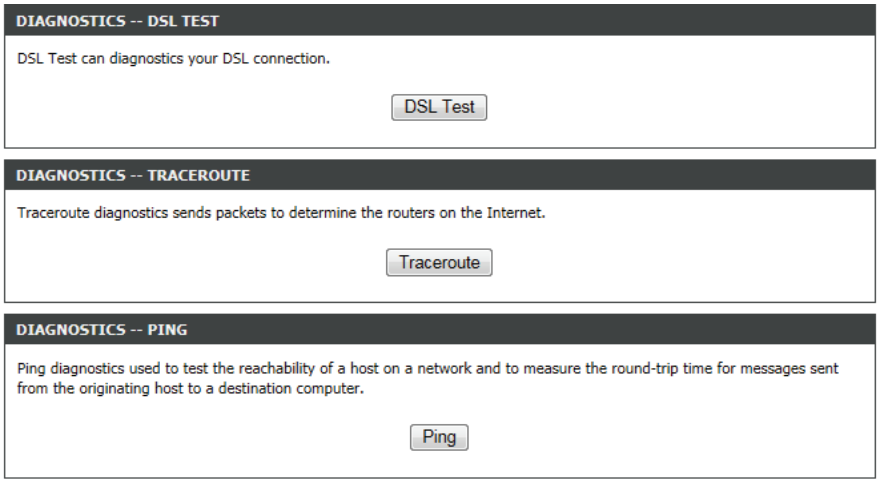
IP Address: Enter an IP Address to be added to the ACL.


IP ADDRESS
The IP Address Access Control mode, if enabled, permits access to local management services from IP addresses contained in the Access Control List. If the Access Control mode is disabled, the system will not validate IP adresses for incoming packets. The services are the system applications listed in the Service Control List.
Enter the IP address of the management station permitted to access the local management services, and click "Apply".
ACCESS CONTROL -- IP ADDRESSES
Enable Access Control Mode
IP
Add
Delete
IP ADDRESS
IP Address :
Apply
Cancel

Diagnosis

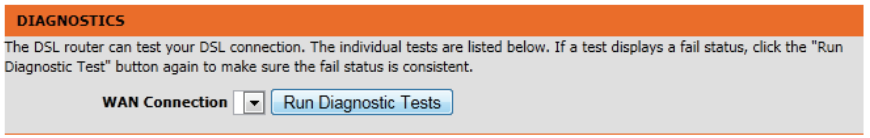
The Diagnosis section provides various method of testing your router and network.

Click the **DSL Test**, **Traceroute**, or **Ping** buttons, to reveal the associated configuration options.


DIAGNOSTICS -- DSL TEST
DSL Test can diagnostics your DSL connection.
DSL Test
DIAGNOSTICS -- TRACEROUTE
Traceroute diagnostics sends packets to determine the routers on the Internet.
Traceroute
DIAGNOSTICS -- PING
Ping diagnostics used to test the reachability of a host on a network and to measure the round-trip time for messages sent from the originating host to a destination computer.
Ping

DSL Test

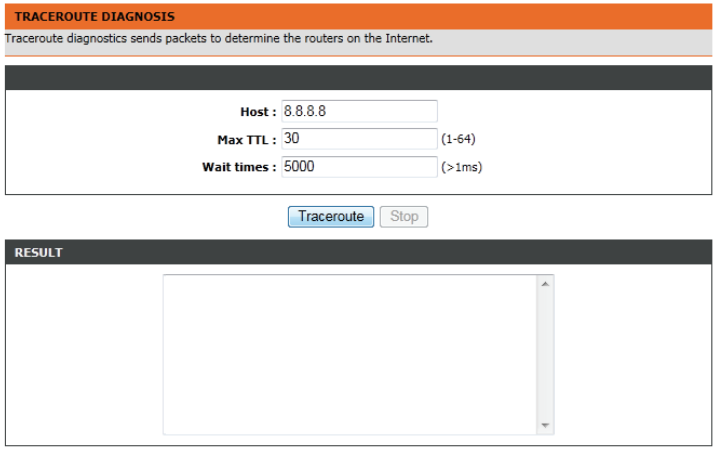
The DSL section provides a way for you to test your DSL connection.


DIAGNOSTICS
The DSL router can test your DSL connection. The individual tests are listed below. If a test displays a fail status, click the "Run Diagnostic Test" button again to make sure the fail status is consistent.
WAN Connection
Run Diagnostic Tests

WAN Connection: Select the connection from the dropdown menu that you would like to test.

Traceroute

The Traceroute section enables you to run a traceroute test.



Host: Enter a host to run a traceroute against.

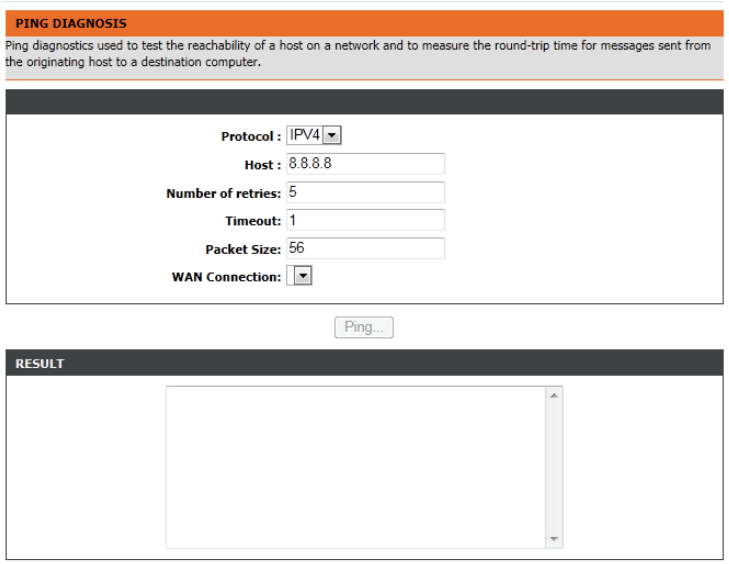
Max TTL: Enter a maximum value for TTL.

Wait times: Enter a maximum value for wait times between hops.

Result: The results of the traceroute test will be displayed here.

Ping

The Ping section enables you to run a ping test.


PING DIAGNOSIS
Ping diagnostics used to test the reachability of a host on a network and to measure the round-trip time for messages sent from the originating host to a destination computer.
Protocol : IPV4
Host : 8.8.8.8
Number of retries: 5
Timeout: 1
Packet Size: 56
WAN Connection:
Ping...
RESULT

Protocol: Select which protocol you would like to use for the ping test.

Host: Enter a host to ping.

Number of retries: Enter a value for the number of time you would like to ping the host.

Timeout: Enter a timeout value before a failure is declared.

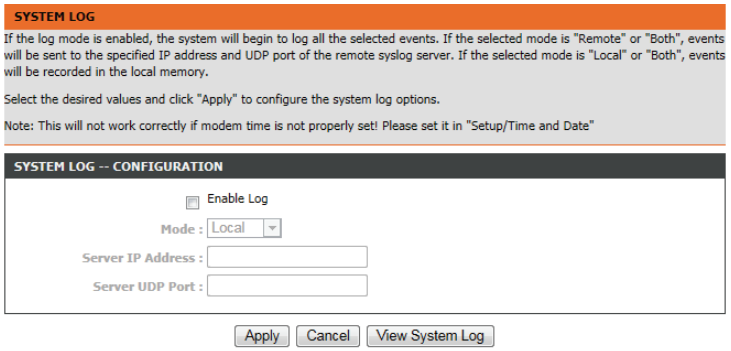
Packet Size: Enter a value for the ping packet size.

WAN Connection: Select a WAN connection from the dropdown menu to use for the ping test

Result: The results of the ping test will be displayed here.

Log Configuration

The GO-DSL-AC750 keeps a running log of events and activities occurring on the Router. You may send these logs to a SysLog server on your network. You can view the current log by clicking the **View System Log** button.


SYSTEM LOG
If the log mode is enabled, the system will begin to log all the selected events. If the selected mode is "Remote" or "Both", events will be sent to the specified IP address and UDP port of the remote syslog server. If the selected mode is "Local" or "Both", events will be recorded in the local memory.
Select the desired values and click "Apply" to configure the system log options.
Note: This will not work correctly if modem time is not properly set! Please set it in "Setup/Time and Date"
SYSTEM LOG -- CONFIGURATION
Enable Log
Mode : Local
Server IP Address :
Server UDP Port :
Apply
Cancel
View System Log

Enable Log: Check to enable or disable logging

Mode: Select to record the log to **Local**, **Remote**, or **Both**.

Server IP Address: Enter an IP address for the remote logging server.

Server UDP Port: Enter the UDP port of the remote server.

Status

Device Info

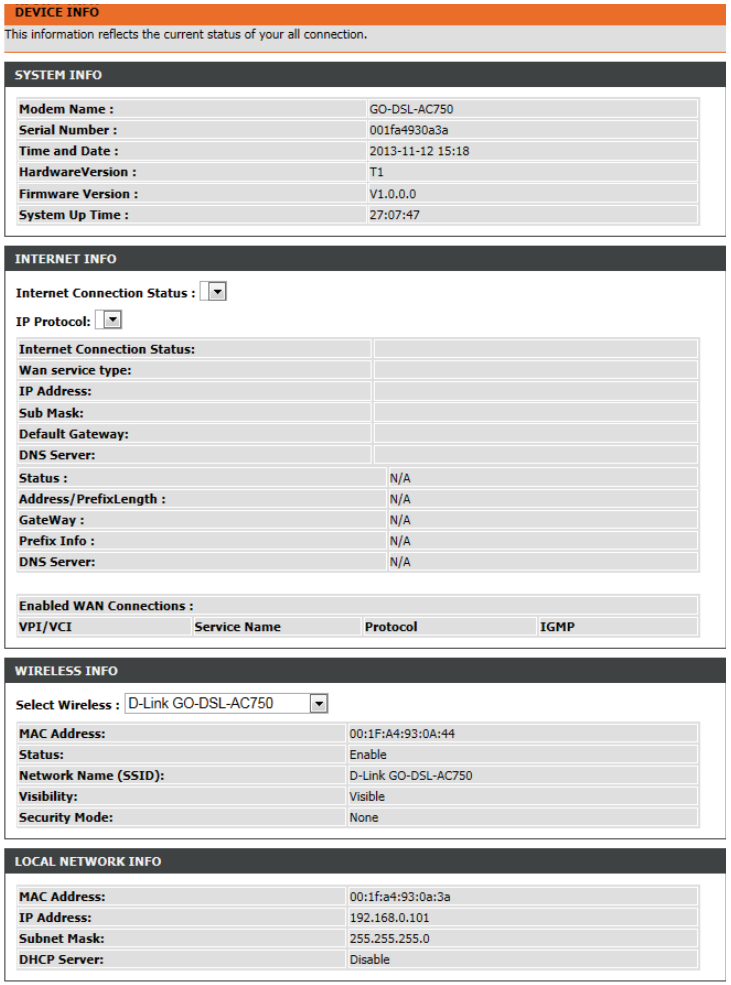
This page displays the current information for the GO-DSL-AC750, such as LAN and wireless LAN information and statistics.

System Info: This section displays a summary of the System settings

Internet Info: This section displays of the internet connection settings.

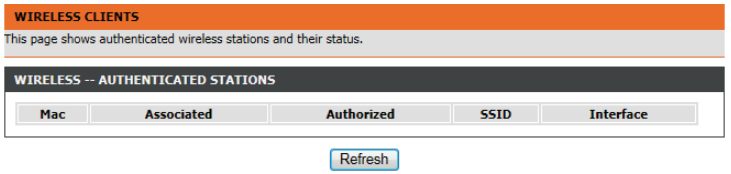
Wireless Info: This section displays a summary of the wireless network setttings.

Local Network Info: This section displays a summary of the LAN settings.



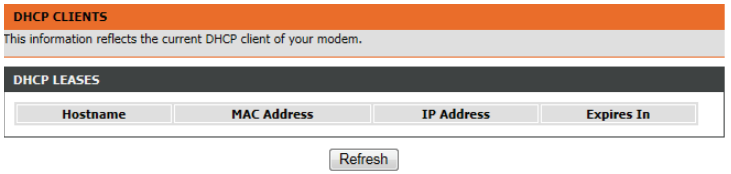
Wireless Clients

The wireless section allows you to view the wireless clients that are connected to your wireless networks.



DHCP Clients

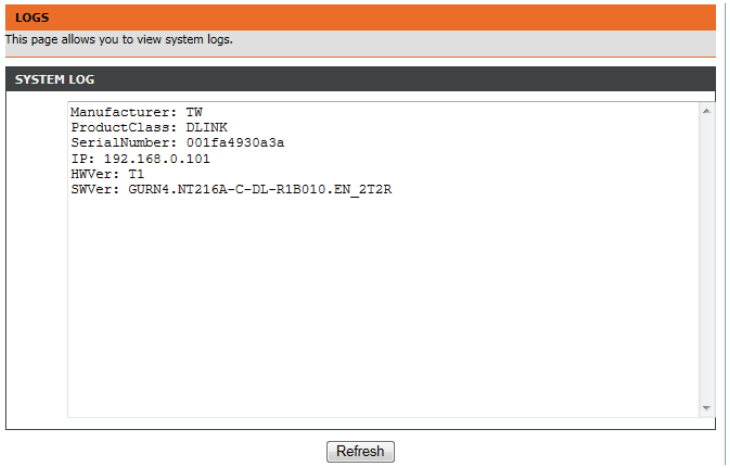
The DHCP Clients section allows you to view the clients that are connected to your router using DCHP.



Logs

The GO-DSL-AC750 keeps a running log of events and activities occurring on the router. If the device is rebooted, the logs will automatically be cleared.

The router automatically logs (records) events of possible interest in it's internal memory. If there isn't enough internal memory for all events, logs of older events are deleted but logs of the latest events are retained. The Logs option allows you to view the router logs. You can define what types of events you want to view and the level of the events to view. This router also has external Syslog Server support so you can send the log files to a computer on your network that is running a Syslog utility.



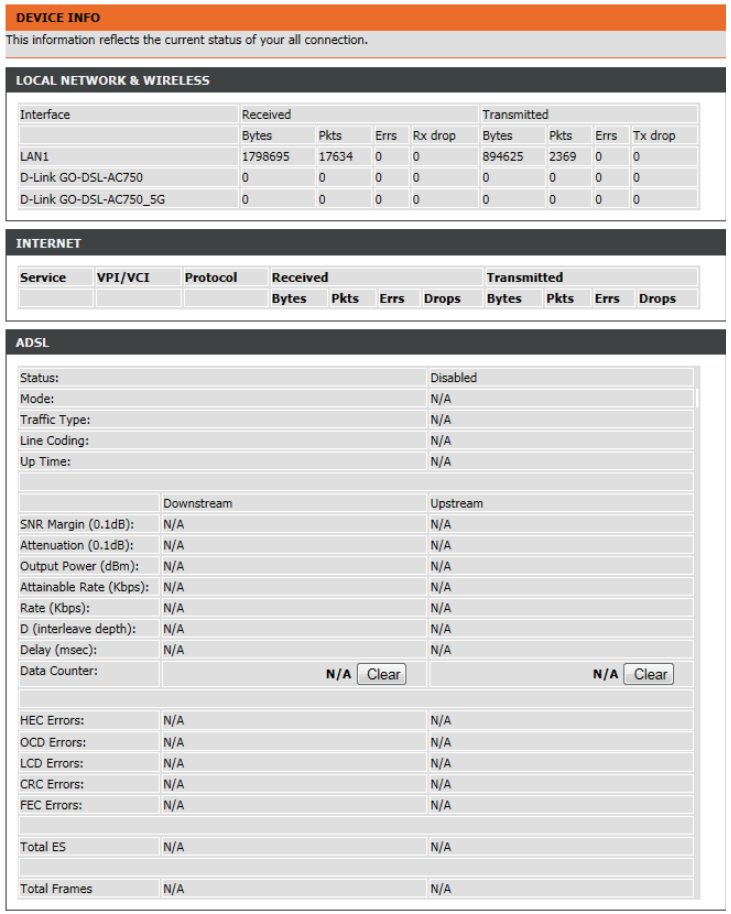
Statistics

The GO-DSL-AC750 keeps statistics of the traffic that passes through it. You can view the amount of packets that pass through the LAN and wireless portions of the network. The traffic counter will reset if the router point is rebooted.

Local Network & Wireless Info: This section displays a statistical summary of the LAN and wireless interfaces.

Internet: This section displays a statistical summary of the internet connection.

ADSL: This section displays a statistical summary of the ADSL interface.



DEVICE INFO

This information reflects the current status of your all connection.

LOCAL NETWORK & WIRELESS

Interface	Received				Transmitted			
	Bytes	Pkts	Errs	Rx drop	Bytes	Pkts	Errs	Tx drop
LAN1	1798695	17634	0	0	894625	2369	0	0
D-Link GO-DSL-AC750	0	0	0	0	0	0	0	0
D-Link GO-DSL-AC750_5G	0	0	0	0	0	0	0	0

INTERNET

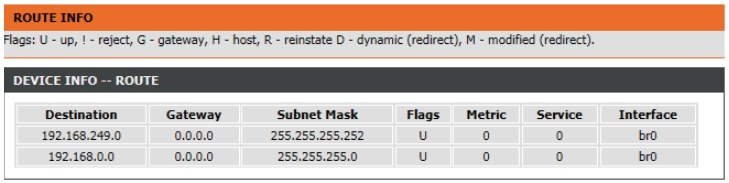
Service	VPI/VCI	Protocol	Received				Transmitted			
			Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops

ADSL

Status:		Disabled
Mode:		N/A
Traffic Type:		N/A
Line Coding:		N/A
Up Time:		N/A
	Downstream	Upstream
SNR Margin (0.1dB):	N/A	N/A
Attenuation (0.1dB):	N/A	N/A
Output Power (dBm):	N/A	N/A
Attainable Rate (Kbps):	N/A	N/A
Rate (Kbps):	N/A	N/A
D (interleave depth):	N/A	N/A
Delay (msec):	N/A	N/A
Data Counter:	N/A Clear	N/A Clear
HEC Errors:	N/A	N/A
OCD Errors:	N/A	N/A
LCD Errors:	N/A	N/A
CRC Errors:	N/A	N/A
FEC Errors:	N/A	N/A
Total ES	N/A	N/A
Total Frames	N/A	N/A

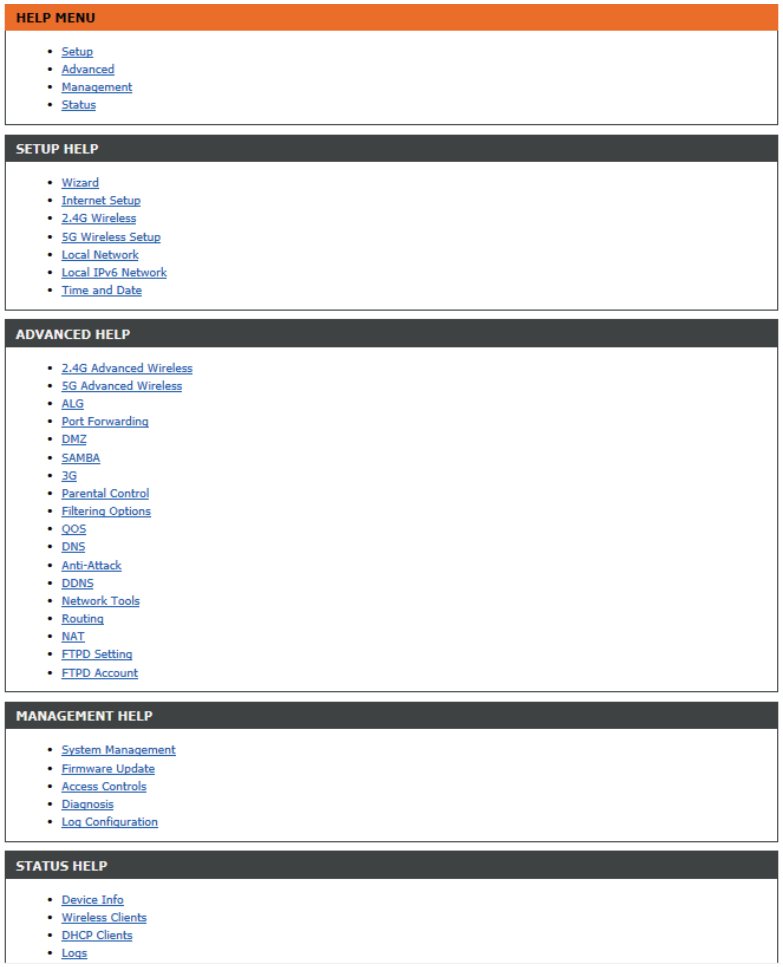
Route Info

The Route Info page displays a summary of the current route configuration between the router and the WAN.


ROUTE INFO
Flags: U - up, ! - reject, G - gateway, H - host, R - reinstate D - dynamic (redirect), M - modified (redirect).
DEVICE INFO -- ROUTE
Destination Gateway Subnet Mask Flags Metric Service Interface
192.168.249.0 0.0.0.0 255.255.255.252 U 0 0 br0
192.168.0.0 0.0.0.0 255.255.255.0 U 0 0 br0

Help

This page provides help and explanations for different sections of the firmware.

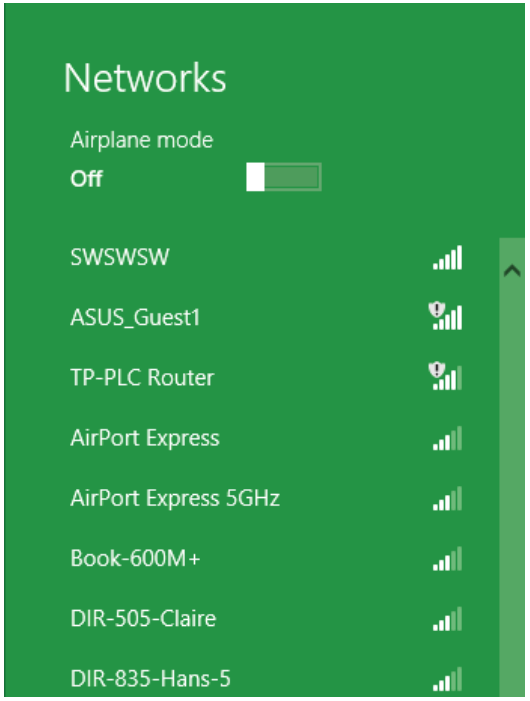


Connecting To Your Wireless Network
Windows® 8
WPA/WPA2

It is recommended to enable wireless security (WPA/WPA2) on your wireless router or access point before configuring your wireless adapter. If you are joining an existing network, you will need to know the security key (Wi-Fi password) being used.

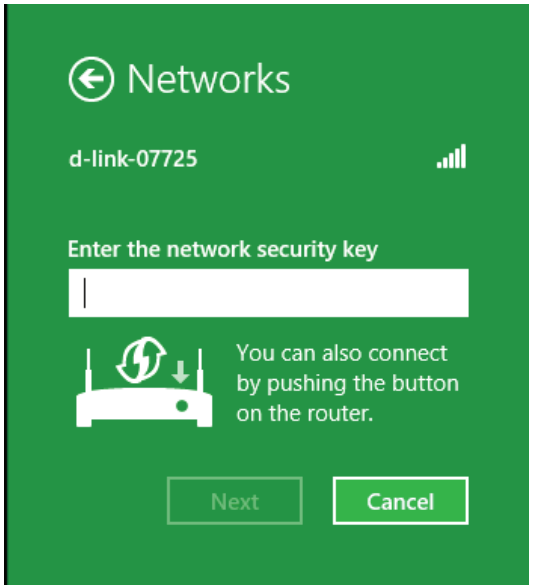
To join an existing network, locate the wireless network icon in the taskbar, next to the time display.

Clicking on this icon will display a list of wireless networks which are within connecting proximity of your computer. Select the desired network by clicking on the network name.

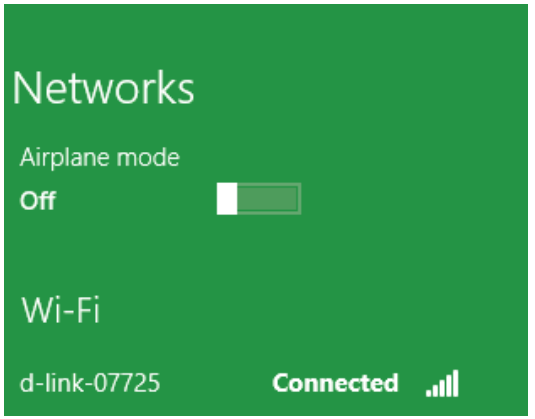


You will then be prompted to enter the network security key (Wi-Fi password) for the wireless network. Enter the password into the box and click **Next**.

If you wish to use Wi-Fi Protected Setup (WPS) to connect to the router, you can also press the WPS button on your router at the point to enable the WPS function.



When you have established a successful connection a wireless network, the word **Connected** will appear next to the name of the network to which you are connected.



Windows® 7
WPA/WPA2

It is recommended to enable wireless security (WPA/WPA2) on your wireless router or access point before configuring your wireless adapter. If you are joining an existing network, you will need to know the security key or passphrase being used.

1. Click on the wireless icon in your system tray (lower-right corner).

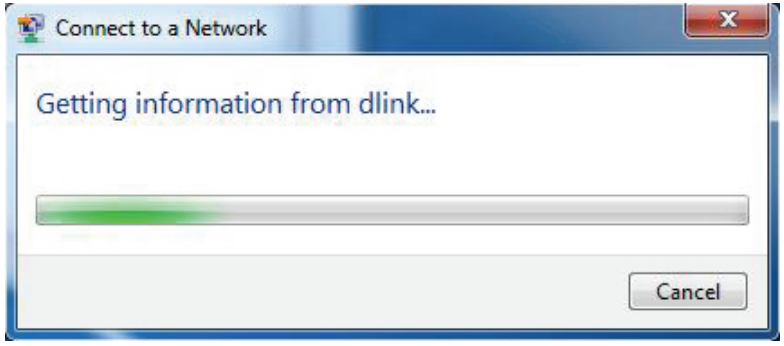
Wireless Icon

2. The utility will display any available wireless networks in your area.

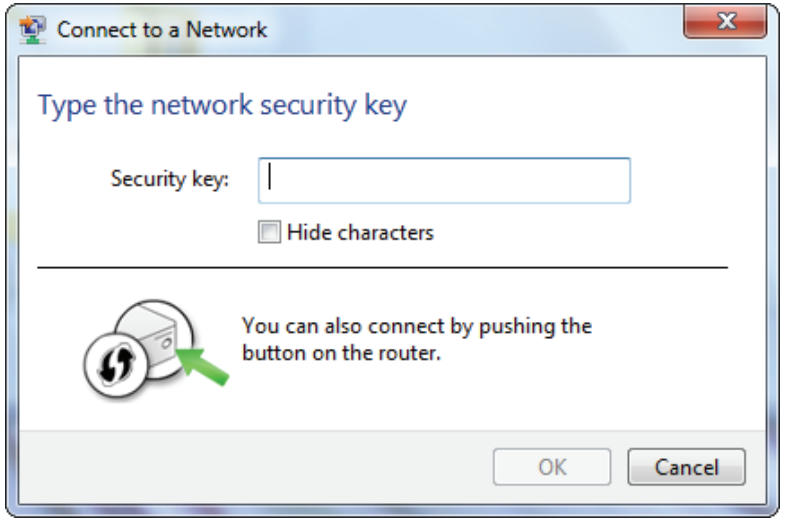
3. Highlight the wireless connection with Wi-Fi name (SSID) you would like to connect to and click the **Connect** button.

   If you get a good signal but cannot access the Internet, check your TCP/IP settings for your wireless adapter. Refer to the Networking Basics section in this manual for more information.

4. The following window appears while your computer tries to connect to the router.



5. Enter the same security key or passphrase (Wi-Fi password) that is on your router and click **Connect**. You can also connect by pushing the WPS button on the router.

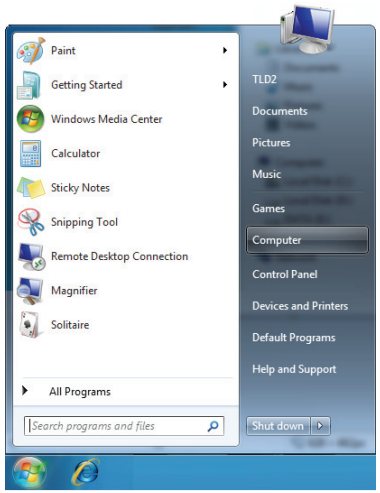


It may take 20-30 seconds to connect to the wireless network. If the connection fails, please verify that the security settings are correct. The key or passphrase must be exactly the same as on the wireless router.

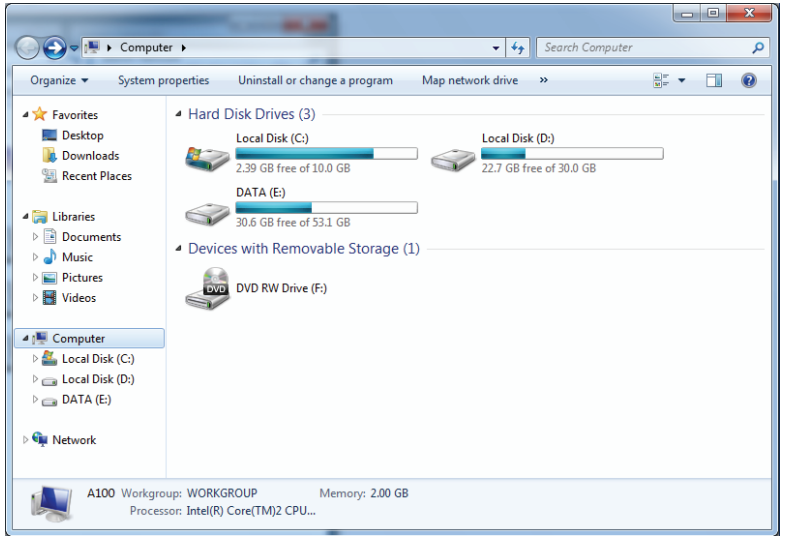
WPS

The WPS feature of the GO-DSL-AC750 can be configured using Windows® 7. Carry out the following steps to use Windows® 7 to configure the WPS feature:

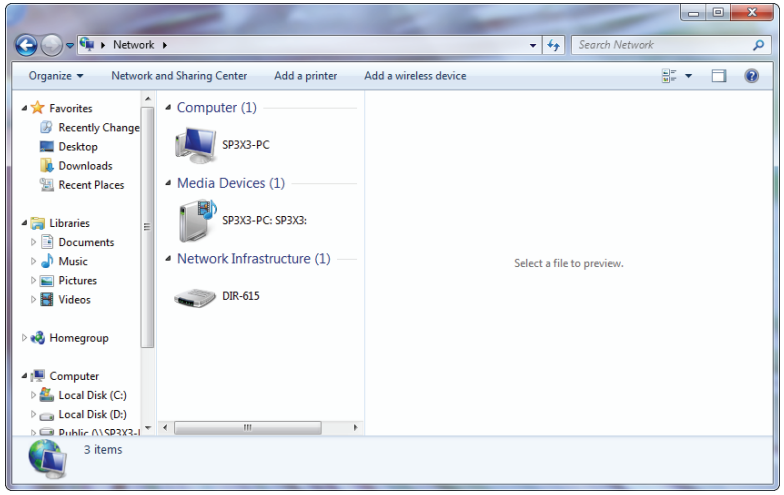
1. Click the **Start** button and select **Computer** from the Start menu.



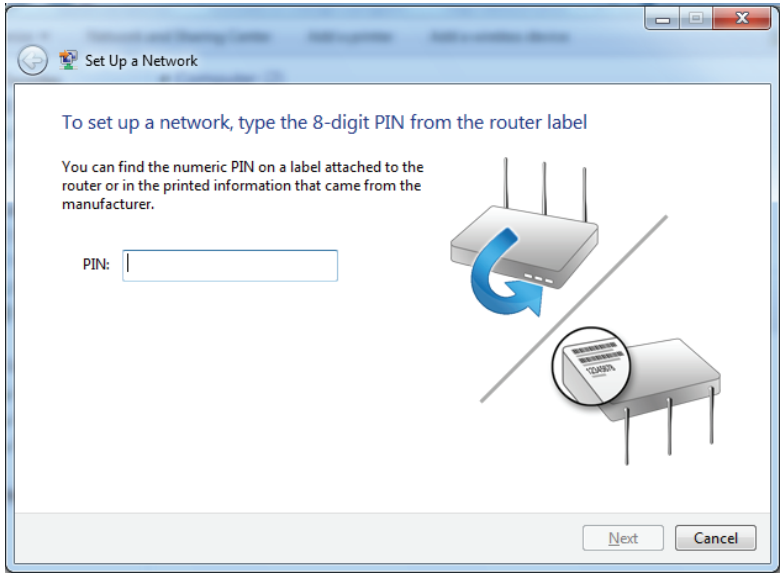
2. Click **Network** on the left side.



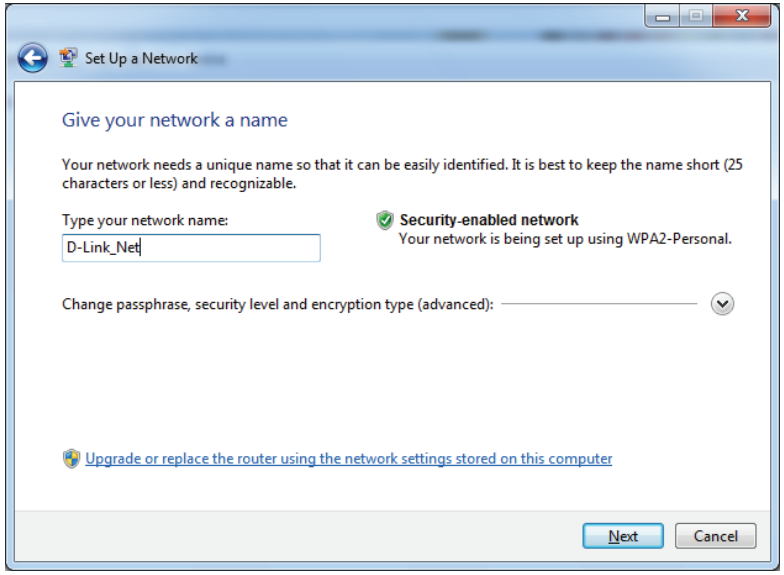
3. Double-click the GO-DSL-AC750.



4. Input the WPS PIN number (on the router label) in the **Setup** > **Wireless Setup** menu in the Router's Web UI) and click **Next**.

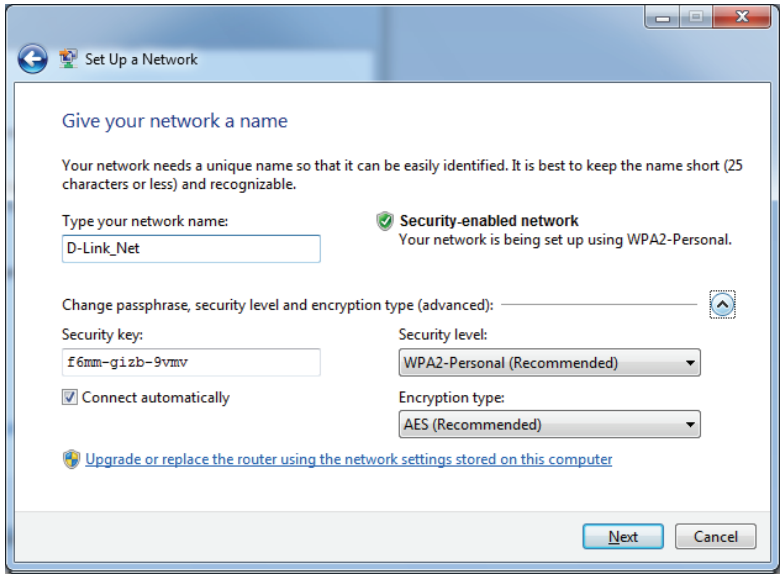

Set Up a Network
To set up a network, type the 8-digit PIN from the router label
You can find the numeric PIN on a label attached to the router or in the printed information that came from the manufacturer.
PIN:
Next
Cancel

5. Type a name to identify the network.


Set Up a Network
Give your network a name
Your network needs a unique name so that it can be easily identified. It is best to keep the name short (25 characters or less) and recognizable.
Type your network name:
D-Link_Net
Security-enabled network
Your network is being set up using WPA2-Personal.
Change passphrase, security level and encryption type (advanced):
Upgrade or replace the router using the network settings stored on this computer
Next
Cancel

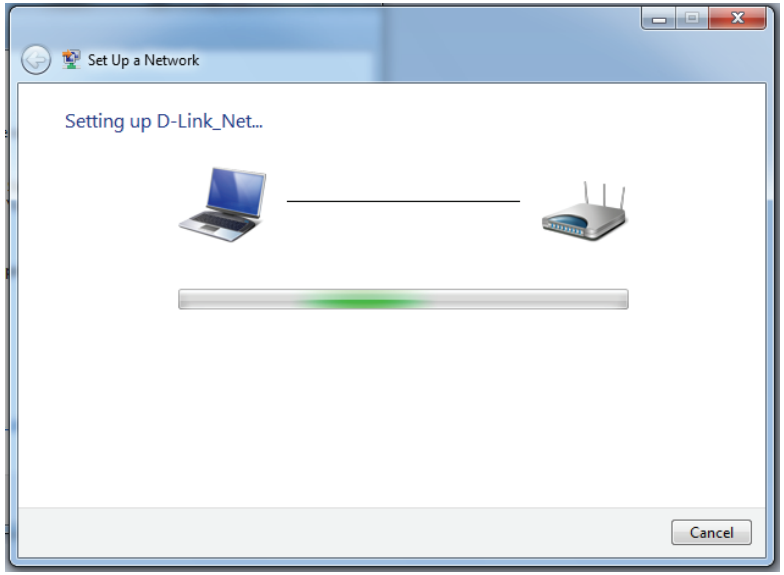
6. To configure advanced settings, click the icon.

Click **Next** to continue.


Set Up a Network
Give your network a name
Your network needs a unique name so that it can be easily identified. It is best to keep the name short (25 characters or less) and recognizable.
Type your network name:
D-Link_Net
Security-enabled network
Your network is being set up using WPA2-Personal.
Change passphrase, security level and encryption type (advanced):
Security key:
f6mm-gizb-9vmv
Security level:
WPA2-Personal (Recommended)
Connect automatically
Encryption type:
AES (Recommended)
Upgrade or replace the router using the network settings stored on this computer
Next
Cancel

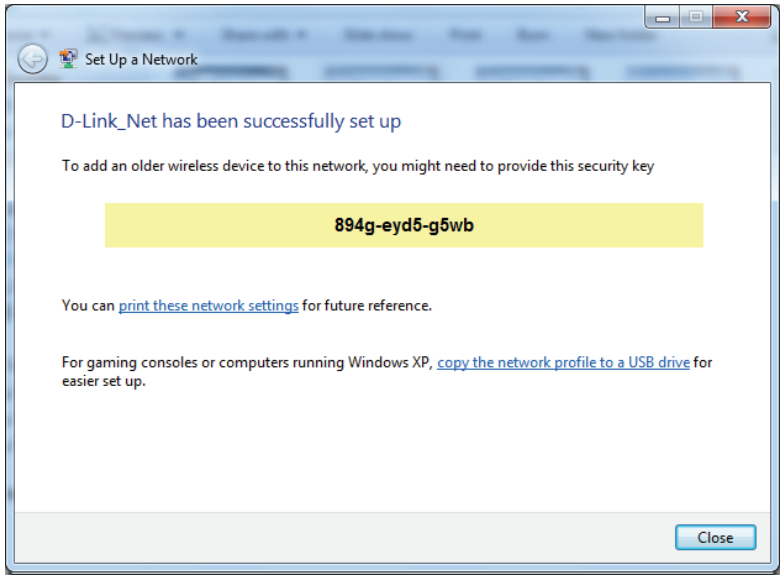
7. The following window appears while the Router is being configured.

   Wait for the configuration to complete.



8. The following window informs you that WPS on the router has been setup successfully.

   Make a note of the security key as you may need to provide this security key if adding an older wireless device to the network in the future.


Set Up a Network
D-Link_Net has been successfully set up
To add an older wireless device to this network, you might need to provide this security key
894g-eyd5-g5wb
You can print these network settings for future reference.
For gaming consoles or computers running Windows XP, copy the network profile to a USB drive for easier set up.
Close

9. Click **Close** to complete WPS setup.

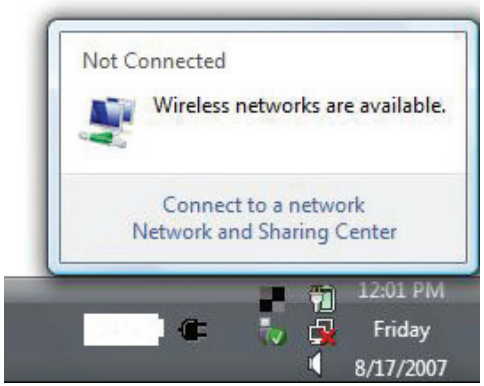
Windows Vista®

Windows Vista® users may use the built-in wireless utility. If you are using another company's utility, please refer to the user manual of your wireless adapter for help with connecting to a wireless network. Most utilities will have a "site survey" option similar to the Windows Vista® utility as seen below.

If you receive the **Wireless Networks Detected** bubble, click on the center of the bubble to access the utility.

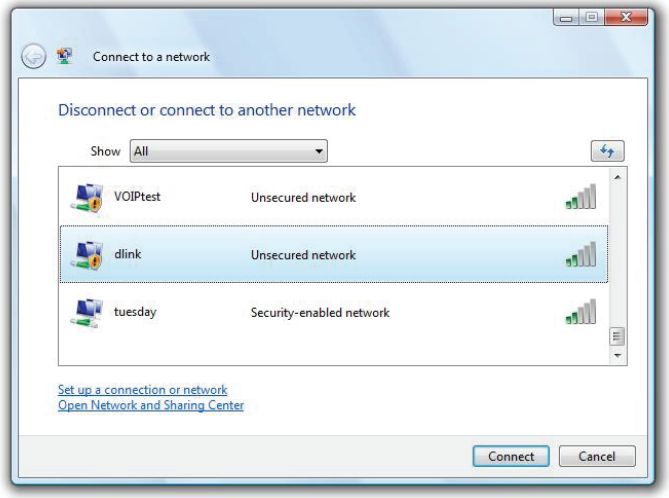
or

Right-click on the wireless computer icon in your system tray (lower-right corner next to the time). Select **Connect to a network**.



The utility will display any available wireless networks in your area. Click on a network (displayed using the SSID) and click the **Connect** button.

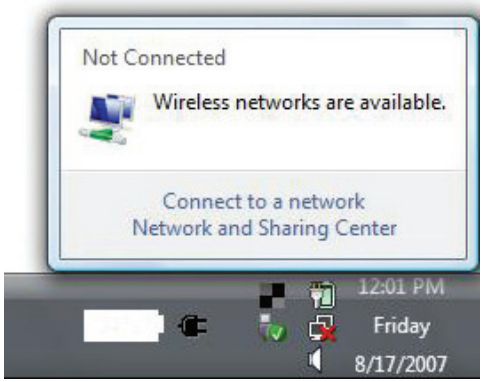
If you get a good signal but cannot access the Internet, check you TCP/IP settings for your wireless adapter. Refer to the **Networking Basics** section in this manual for more information.



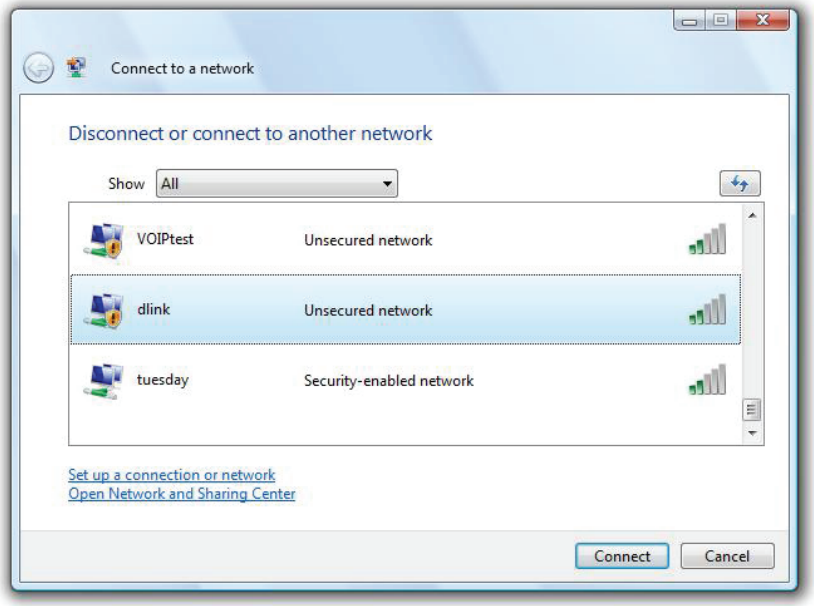
WPA/WPA2

It is recommended to enable wireless security (WPA/WPA2) on your wireless router or access point before configuring your wireless adapter. If you are joining an existing network, you will need to know the security key or passphrase being used.

1. Open the Windows Vista® Wireless Utility by right-clicking on the wireless computer icon in your system tray (lower right corner of screen). Select **Connect to a network**.



2. Highlight the Wi-Fi name (SSID) you would like to connect to and click **Connect**.



3. Enter the same security key or passphrase (Wi-Fi password) that is on your router and click **Connect**.

It may take 20-30 seconds to connect to the wireless network. If the connection fails, please verify that the security settings are correct. The key or passphrase must be exactly the same as on the wireless router.

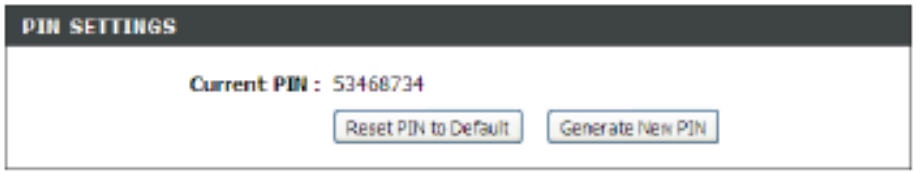
Connect to a network
Type the network security key or passphrase for Candy
The person who setup the network can give you the key or passphrase.
Security key or passphrase:
Display characters
If you have a USB flash drive with network settings for Candy, insert it now.
Connect
Cancel

WPS/WCN 2.0

The router supports Wi-Fi protection, referred to as WCN 2.0 in Windows Vista®. The following instructions for setting this up depends on whether you are using Windows Vista® to configure the router or third party software.

When you first set up the router, Wi-Fi protection is disabled and unconfigured. To enjoy the benefits of Wi-Fi protection, the router must be both enabled and configured. There are three basic methods to accomplish this: use Windows Vista's built-in support for WCN 2.0, use software provided by a third party, or manually configure.

If you are running Windows Vista®, log into the router and click the **Enable** checkbox in the **Basic** > **Wireless** section. Use the Current PIN that is displayed on the **Advanced** > **Wi-Fi Protected Setup** section or choose to click the **Generate New PIN** button or **Reset PIN to Default** button.

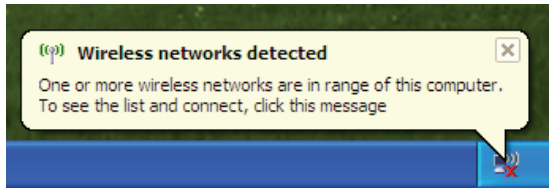


If you are using third party software to set up Wi-Fi Protection, carefully follow the directions. When you are finished, proceed to the next section to set up the newly-configured router.

Windows® XP

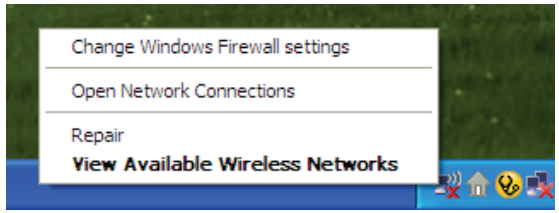
Windows® XP users may use the built-in wireless utility (Zero Configuration Utility). The following instructions are for Service Pack 2 users. If you are using another company's utility, please refer to the user manual of your wireless adapter for help with connecting to a wireless network. Most utilities will have a "site survey" option similar to the Windows® XP utility as seen below.

If you receive the **Wireless Networks Detected** bubble, click on the center of the bubble to access the utility.


Wireless networks detected
One or more wireless networks are in range of this computer.
To see the list and connect, click this message

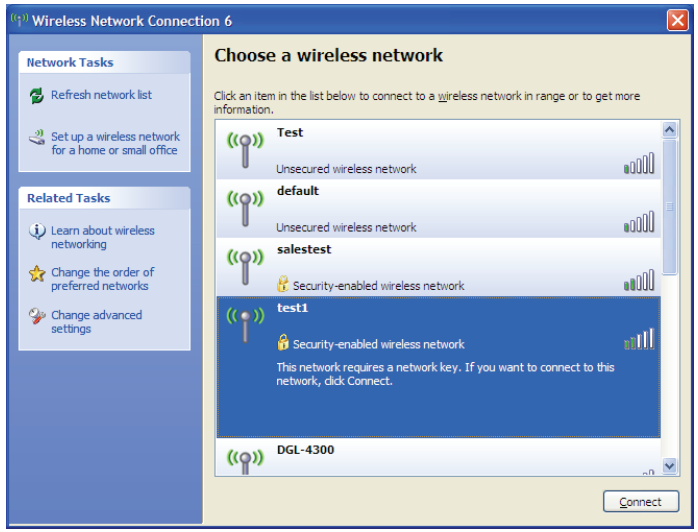
or

Right-click on the wireless computer icon in your system tray (lower-right corner next to the time). Select **View Available Wireless Networks**.



The utility will display any available wireless networks in your area. Click on a Wi-Fi network (displayed using the SSID) and click the **Connect** button.

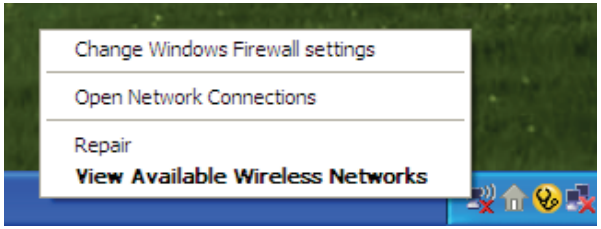
If you get a good signal but cannot access the Internet, check you TCP/IP settings for your wireless adapter. Refer to the **Networking Basics** section in this manual for more information.


Wireless Network Connection 6
Network Tasks
Refresh network list
Set up a wireless network for a home or small office
Related Tasks
Learn about wireless networking
Change the order of preferred networks
Change advanced settings
Choose a wireless network
Click an item in the list below to connect to a wireless network in range or to get more information.
Test
Unsecured wireless network
default
Unsecured wireless network
salestest
Security-enabled wireless network
test1
Security-enabled wireless network
This network requires a network key. If you want to connect to this network, click Connect.
DGL-4300
Connect

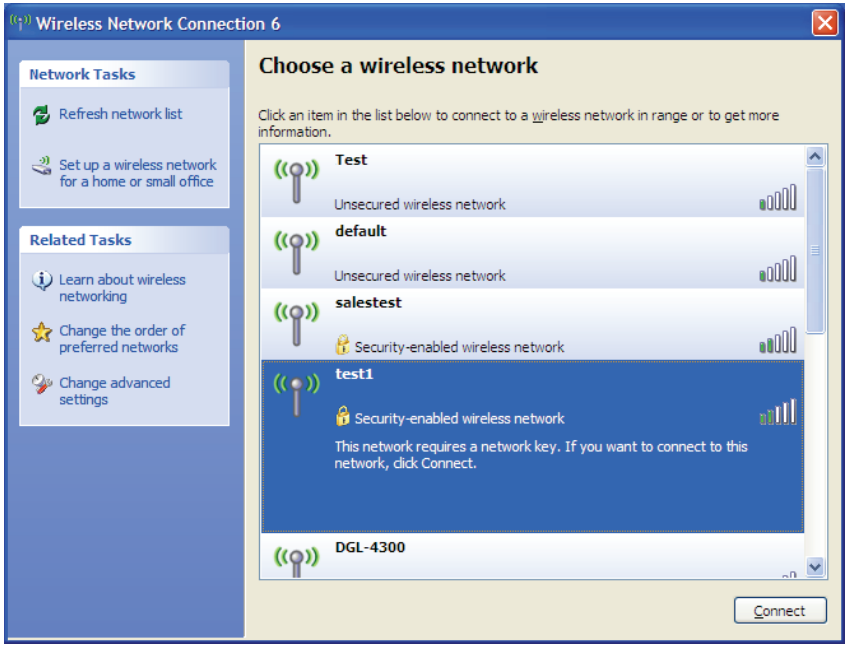
WPA/WPA2

It is recommended to enable WPA on your wireless router or access point before configuring your wireless adapter. If you are joining an existing network, you will need to know the WPA key being used.

1. Open the Windows® XP Wireless Utility by right-clicking on the wireless computer icon in your system tray (lower-right corner of screen). Select **View Available Wireless Networks**.

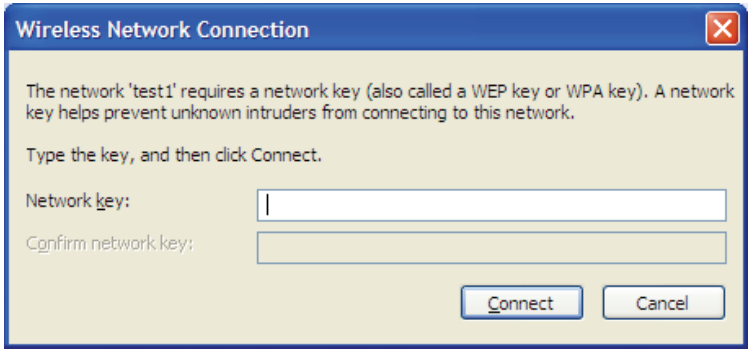


2. Highlight the Wi-Fi network (SSID) you would like to connect to and click **Connect**.


Wireless Network Connection 6
Network Tasks
Refresh network list
Set up a wireless network for a home or small office
Related Tasks
Learn about wireless networking
Change the order of preferred networks
Change advanced settings
Choose a wireless network
Click an item in the list below to connect to a wireless network in range or to get more information.
Test
Unsecured wireless network
default
Unsecured wireless network
salestest
Security-enabled wireless network
test1
Security-enabled wireless network
This network requires a network key. If you want to connect to this network, click Connect.
DGL-4300
Connect

3. The **Wireless Network Connection** box will appear. Enter the WPA-PSK Wi-Fi password and click **Connect**.

It may take 20-30 seconds to connect to the wireless network. If the connection fails, please verify that the WPA-PSK settings are correct. The Wi-Fi password must be exactly the same as on the wireless router.


Wireless Network Connection
The network 'test1' requires a network key (also called a WEP key or WPA key). A network key helps prevent unknown intruders from connecting to this network.
Type the key, and then click Connect.
Network key:
Confirm network key:
Connect
Cancel

Troubleshooting

This chapter provides solutions to problems that can occur during the installation and operation of the GO-DSL-AC750. Read the following descriptions if you are having problems. The examples below are illustrated in Windows® XP. If you have a different operating system, the screenshots on your computer will look similar to the following examples.

1. Why can't I access the web-based configuration utility?

When entering the IP address of the D-Link router (192.168.1.1 for example), you are not connecting to a website nor do you have to be connected to the Internet. The device has the utility built-in to a ROM chip in the device itself. Your computer must be on the same IP subnet to connect to the web-based utility.

- Make sure you have an updated Java-enabled web browser. We recommend the following:

  - Microsoft Internet Explorer® 7 and higher
  - Mozilla Firefox 3.5 and higher
  - Google™ Chrome 8 and higher
  - Apple Safari 4 and higher

- Verify physical connectivity by checking for solid link lights on the device. If you do not get a solid link light, try using a different cable or connect to a different port on the device if possible. If the computer is turned off, the link light may not be on.

- Disable any Internet security software running on the computer. Software firewalls such as Zone Alarm, Black Ice, Sygate, Norton Personal Firewall, and Windows® XP firewall may block access to the configuration pages. Check the help files included with your firewall software for more information on disabling or configuring it.

- Configure your Internet settings:
    - Go to **Start** > **Settings** > **Control Panel**. Double-click the **Internet Options** Icon. From the **Security** tab, click the button to restore the settings to their defaults.
    - Click the **Connection** tab and set the dial-up option to Never Dial a Connection. Click the LAN Settings button. Make sure nothing is checked. Click **OK**.
    - Go to the **Advanced** tab and click the button to restore these settings to their defaults. Click **OK** three times.
    - Close your web browser (if open) and open it.
- Access the web management. Open your web browser and enter the IP address of your D-Link router in the address bar. This should open the login page for your web management.
- If you still cannot access the configuration, unplug the power to the router for 10 seconds and plug back in. Wait about 30 seconds and try accessing the configuration. If you have multiple computers, try connecting using a different computer.

2. What can I do if I forgot my password?

If you forgot your password, you must reset your router. Unfortunately this process will change all your settings back to the factory defaults.

To reset the router, locate the reset button (hole) on the rear panel of the unit. With the router powered on, use a paperclip to hold the button down for 10 seconds. Release the button and the router will go through its reboot process. Wait about 30 seconds to access the router. The default IP address is 192.168.1.1. When logging in, the username is **admin** and leave the password box empty.

3. Why can't I connect to certain sites or send and receive emails when connecting through my router?

If you are having a problem sending or receiving email, or connecting to secure sites such as eBay, banking sites, and Hotmail, we suggest lowering the MTU in increments of ten (Ex. 1492, 1482, 1472, etc).

To find the proper MTU Size, you'll have to do a special ping of the destination you're trying to go to. A destination could be another computer, or a URL.

- Click on **Start** and then click **Run**.
- Windows® 95, 98, and Me users type in **command** (Windows® NT, 2000, XP, Vista®, and 7 users type in **cmd**) and press **Enter** (or click **OK**).
- Once the window opens, you'll need to do a special ping. Use the following syntax:

ping [url] [-f] [-l] [MTU value]

Example: **ping yahoo.com -f -l 1472**

```
C:\>ping yahoo.com -f -l 1482

Pinging yahoo.com [66.94.234.13] with 1482 bytes of data:

Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.

Ping statistics for 66.94.234.13:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum =  0ms, Average =  0ms

C:\>ping yahoo.com -f -l 1472

Pinging yahoo.com [66.94.234.13] with 1472 bytes of data:

Reply from 66.94.234.13: bytes=1472 time=93ms TTL=52
Reply from 66.94.234.13: bytes=1472 time=109ms TTL=52
Reply from 66.94.234.13: bytes=1472 time=125ms TTL=52
Reply from 66.94.234.13: bytes=1472 time=203ms TTL=52

Ping statistics for 66.94.234.13:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 93ms, Maximum =  203ms, Average =  132ms

C:\>
```

You should start at 1472 and work your way down by 10 each time. Once you get a reply, go up by 2 until you get a fragmented packet. Take that value and add 28 to the value to account for the various TCP/IP headers. For example, lets say that 1452 was the proper value, the actual MTU size would be 1480, which is the optimum for the network we're working with (1452+28=1480).

Once you find your MTU, you can now configure your router with the proper MTU size.

To change the MTU rate on your router follow the steps below:

- Open your browser, enter the IP address of your router (192.168.1.1) and click **OK**.
- Enter your username (admin) and password (blank by default). Click **OK** to enter the web configuration page for the device.
- Click on **Setup** and then click **Manual Configure**.
- To change the MTU enter the number in the MTU field and click **Save Settings** to save your settings.
- Test your email. If changing the MTU does not resolve the problem, continue changing the MTU in increments of ten.

Wireless Security

This section will show you the different levels of security you can use to protect your data from intruders. The GO-DSL-AC750 offers the following types of security:

- WPA2 (Wi-Fi Protected Access 2)
- WPA (Wi-Fi Protected Access)
- WPA2-PSK (Pre-Shared Key)
- WPA-PSK (Pre-Shared Key)

What is WPA?

WPA (Wi-Fi Protected Access), is a Wi-Fi standard that was designed to improve the security features of WEP (Wired Equivalent Privacy).

The 2 major improvements over WEP:

- Improved data encryption through the Temporal Key Integrity Protocol (TKIP). TKIP scrambles the keys using a hashing algorithm and, by adding an integrity-checking feature, ensures that the keys haven't been tampered with. WPA2 is based on 802.11i and uses Advanced Encryption Standard (AES) instead of TKIP.

- User authentication, which is generally missing in WEP, through the extensible authentication protocol (EAP). WEP regulates access to a wireless network based on a computer's hardware-specific MAC address, which is relatively simple to be sniffed out and stolen. EAP is built on a more secure public-key encryption system to ensure that only authorized network users can access the network.

WPA-PSK/WPA2-PSK uses a passphrase or key to authenticate your wireless connection. The key is an alpha-numeric password between 8 and 63 characters long. The password can include symbols (!?*&_) and spaces. This key must be the exact same key entered on your wireless router or access point.

WPA/WPA2 incorporates user authentication through the Extensible Authentication Protocol (EAP). EAP is built on a more secure public key encryption system to ensure that only authorized network users can access the network.

Networking Basics

Check your IP address

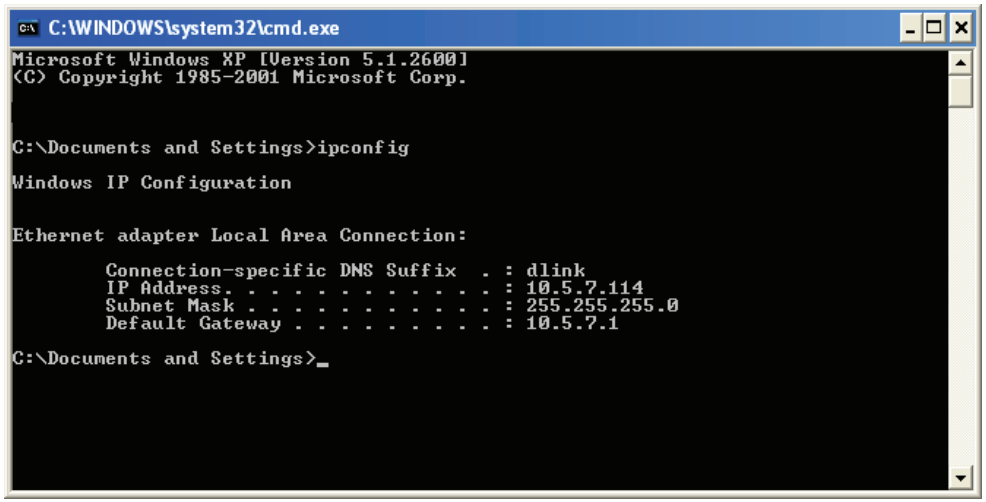
After you install your new D-Link adapter, by default, the TCP/IP settings should be set to obtain an IP address from a DHCP server (i.e. wireless router) automatically. To verify your IP address, please follow the steps below.

Click on **Start** > **Run**. In the run box type ***cmd*** and click **OK.** (Windows® 7/Vista® users type *cmd* in the **Start Search** box.)

At the prompt, type ***ipconfig*** and press **Enter**.

This will display the IP address, subnet mask, and the default gateway of your adapter.

If the address is 0.0.0.0, check your adapter installation, security settings, and the settings on your router. Some firewall software programs may block a DHCP request on newly installed adapters.


C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\Documents and Settings>ipconfig
Windows IP Configuration
Ethernet adapter Local Area Connection:
Connection-specific DNS Suffix . : dlink
IP Address. . . . . : 10.5.7.114
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 10.5.7.1
C:\Documents and Settings>

Statically Assign an IP address

If you are not using a DHCP capable gateway/router, or you need to assign a static IP address, please follow the steps below:

Step 1

Windows® 7 - Click on **Start** > **Control Panel** > **Network and Internet** > **Network and Sharing Center**.

Windows Vista® - Click on **Start** > **Control Panel** > **Network and Internet** > **Network and Sharing Center** > **Manage Network Connections.**

Windows® XP - Click on **Start** > **Control Panel** > **Network Connections**.

Windows® 2000 - From the desktop, right-click **My Network Places** > **Properties**.

Step 2

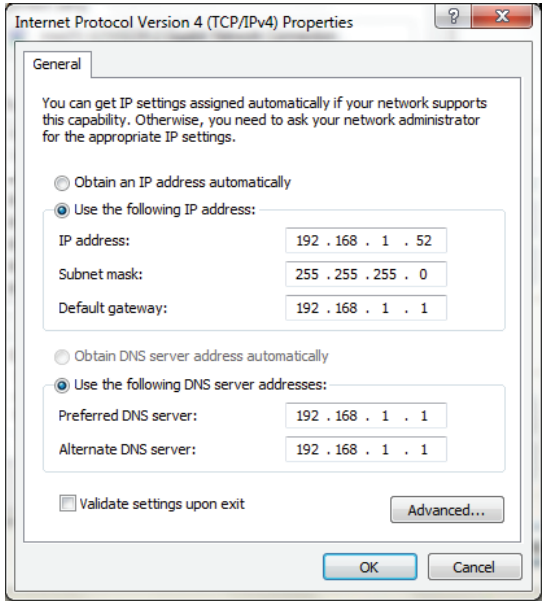
Right-click on the **Local Area Connection** which represents your network adapter and select **Properties**.

Step 3

Highlight **Internet Protocol (TCP/IP)** and click **Properties**.

Step 4

Click **Use the following IP address** and enter an IP address that is on the same subnet as your network or the LAN IP address on your router.


Internet Protocol Version 4 (TCP/IPv4) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address: 192 . 168 . 1 . 52
Subnet mask: 255 . 255 . 255 . 0
Default gateway: 192 . 168 . 1 . 1
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server: 192 . 168 . 1 . 1
Alternate DNS server: 192 . 168 . 1 . 1
Validate settings upon exit
Advanced...
OK
Cancel

Example: If the router´s LAN IP address is 192.168.1.1, make your IP address 192.168.1.X where X is a number between 2 and 99. Make sure that the number you choose is not in use on the network. Set the Default Gateway the same as the LAN IP address of your router (I.E. 192.168.1.1).

Set Primary DNS the same as the LAN IP address of your router (192.168.1.1). The Secondary DNS is not needed or you may enter a DNS server from your ISP.

Step 5

Click **OK** twice to save your settings.

Link'n Print

D-Link Link'n Print allows you to share USB devices such as external storage drives and multifunction printers with other users across your network by simply connecting the device to select D-Link routers. This allows you to use an external storage drive or printer located across your network as if it were connected to your local PC.

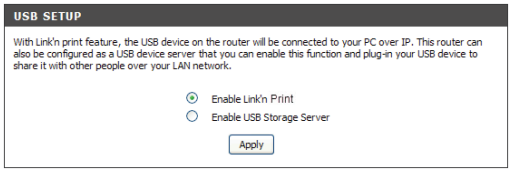
- System Requirements
- Microsoft® Windows
- 2000 / 2003 / XP / Vista / 7 / 8 (32-bit / 64-bit)
- Pentium 3 800MHz or better
- 256MB RAM or higher
- CD-ROM drive
- A compatible D-Link router

Installation

1. Insert the CD-ROM into your computer.
2. Follow the on-screen instructions.
3. The purple icon will appear in the Windows System Tray at the lower-right corner of the desktop and a new icon will be created on the desktop.

Set up the D-Link Router

1. Connect the D-Link Router to the network.
2. Power on the D-Link Router.
3. Double-click on the icon to open D-Link Link'n Print.
4. Right-click on in the System Tray at the lower-right corner on your Windows Desktop. To click on "Configuration…" and a pop up window will display the D-Link Router management GUI.
5. Log in to the router management GUI and navigate to the Net USB page.
6. Select "Enable Link'n Print " and click the "Apply" button.
7. The icon in the Windows System Tray will change to a green icon.


USB SETUP
With Link'n print feature, the USB device on the router will be connected to your PC over IP. This router can also be configured as a USB device server that you can enable this function and plug-in your USB device to share it with other people over your LAN network.
Enable Link'n Print
Enable USB Storage Server
Apply

Connect USB Devices to the D-Link Router

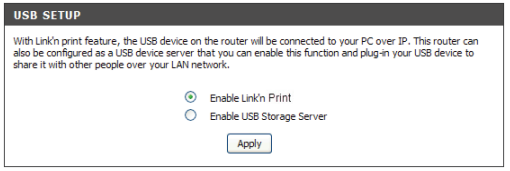
USB SETUP
With Link'n print feature, the USB device on the router will be connected to your PC over IP. This router can also be configured as a USB device server that you can enable this function and plug-in your USB device to share it with other people over your LAN network.
Enable Link'n Print
Enable USB Storage Server
Apply

The D-Link Link'n Print automatically detects for each connected USB device. A window will pop up for each detected USB device.

1. Right-click on the Windows System Tray icon.
2. Click on Open D-Link Link'n Print.
3. The D-Link Link'n Print displays the connected USB devices on the network. To click "Connect" to have the USB device connected.
4. Advanced Options can be set by clicking on Advanced Options.

USB SETUP
With Link'n print feature, the USB device on the router will be connected to your PC over IP. This router can also be configured as a USB device server that you can enable this function and plug-in your USB device to share it with other people over your LAN network.
Enable Link'n Print
Enable USB Storage Server
Apply

Virtually Connect or Disconnect a USB Device


USB SETUP
With Link'n print feature, the USB device on the router will be connected to your PC over IP. This router can also be configured as a USB device server that you can enable this function and plug-in your USB device to share it with other people over your LAN network.
Enable Link'n Print
Enable USB Storage Server
Apply

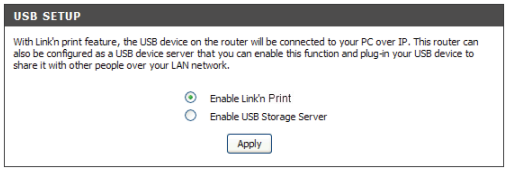
1. Move the cursor to Waiting to Connect and click on Connect to virtually connect a USB device.
2. The D-Link Link'n Print displays which user is virtually connecting this USB device.
3. Move the cursor to In Use By (Owner) and click on Disconnect to virtually disconnect the USB device.

When the USB Device is a Multifunction Printer

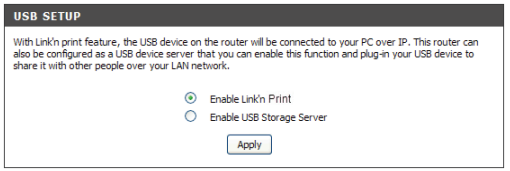
1. Move the cursor to Waiting to Connect and click on Manage Device.

USB SETUP
With Link'n print feature, the USB device on the router will be connected to your PC over IP. This router can also be configured as a USB device server that you can enable this function and plug-in your USB device to share it with other people over your LAN network.
Enable Link'n Print
Enable USB Storage Server
Apply

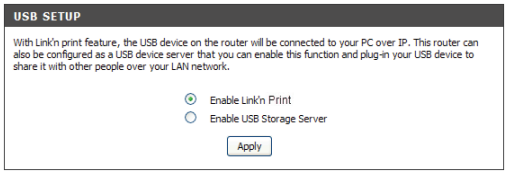
2. Click Yes on the question "Do you want to install the printer software or MFP utility?"


USB SETUP
With Link'n print feature, the USB device on the router will be connected to your PC over IP. This router can also be configured as a USB device server that you can enable this function and plug-in your USB device to share it with other people over your LAN network.
Enable Link'n Print
Enable USB Storage Server
Apply

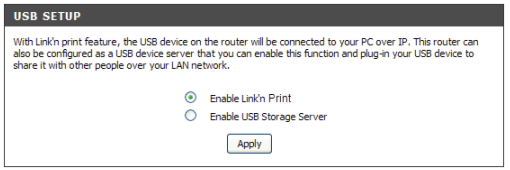
3. Insert the CD-ROM of the multifunction printer and follow the instructions to install the multifunction printer's driver. When the installation process prompts you to connect the multifunction printer to your PC, click Next.


USB SETUP
With Link'n print feature, the USB device on the router will be connected to your PC over IP. This router can also be configured as a USB device server that you can enable this function and plug-in your USB device to share it with other people over your LAN network.
Enable Link'n Print
Enable USB Storage Server
Apply

4. The D-Link Link'n Print virtually connects to this multifunction printer. Click Next


USB SETUP
With Link'n print feature, the USB device on the router will be connected to your PC over IP. This router can also be configured as a USB device server that you can enable this function and plug-in your USB device to share it with other people over your LAN network.
Enable Link'n Print
Enable USB Storage Server
Apply

5. Choose the printer driver that you want D-Link Link'n Print to auto-connect when you print.


USB SETUP
With Link'n print feature, the USB device on the router will be connected to your PC over IP. This router can also be configured as a USB device server that you can enable this function and plug-in your USB device to share it with other people over your LAN network.
Enable Link'n Print
Enable USB Storage Server
Apply

When You Want to Scan

1. Move the cursor to Available for Use and click on Scan Now.

USB SETUP
With LinkN print feature, the USB device on the router will be connected to your PC over IP. The router can also be configured as a USB device server that you can enable this function and plug-in your USB device to share it with other people over your LAN network.
Enable LinkN Print
Enable USB Storage Server
Apply

Technical Specifications

General		
Device Interfaces	• 802.11 ac/n/g/b Wireless LAN • Four 10/100/1000 Gigabit LAN ports	• RJ-11 ADSL port • USB 2.0 port

ADSL Standards	• ADSL 2+ Standards
	  • ITU-T G.992.5 Annex B/J
	• ADSL 2 Standards
	  • ITU-T G.992.3 (G.dmt.bis) Annex B/J
	  • IUU-T G992.4 (G.lite.bis)
		• ADSL Stadards
		  • Full-rate ANSI T1.413 Issue 2
		  • ITU-TG.992.1 (G.dmt) Annex B
		  • ITU-TG.992.2 (G.lite) Annex B
		  • ITU-T G.994.1 (G.hs)

ATM/PPP Support	• Multiprotocol over AAL5 (RFC 1483/2684) • Bridged and routed Ethernet encapsulation • LLC encapsulation • VC-based multiplexing • ATM Forum UNI3.1/4.0 PVC (up to 8 PVCs) • ATM Cell Format ITU-T Rec. I.361 • ATM Adaption Layer Type 5 (AAL5)	• PPPoA (RFC2364) • PPPoE (RFC2516) • PPP Link Control Protocol (RFC 1661) • Internet Protocol Control Protocol (RFC 1332) • PPP Authentication Protocol (RFC 1334) • PPP Challenge Handshake Authentication Protocol (RFC 1994) • Microsoft PPP CHAP extensions (RFC 2433)
WLAN Specifications	• 802.11 n/g/b, up to 150 Mbps • Wi-Fi Protected Setup (WPS) • Multiple SSIDs • Automatic rate adapting • WAN scheduling	• Auto channel selection • WMM support • 64-bit & 128-bit WEP • WPA-PSK & WPA2-PSK • MAC address filtering

Network Services	• IPv4
	• DHCP server/client/relay
	• DNS relay
	• Dynamic DNS (DDNS)
	• Routing Information Protocol (RIP) v1/v2
	• NAT AGLs
	  • PPTP
	  • L2TP
	  • FTP
	  • RTSP (RealTime Streaming Protocol)
	  • SIP v1/v2
	  • IPsec
	• Internet Control Message Protocol (ICMP)
	• Virtual server (Port forwarding)
		• Simple Network Time Protocol (SNTP)
		• 802.1d MAC Bridge (up to 256*8 MAC addresses)
		• QoS
		  • IPP/ToS
		  • DSCP QoS in 4-priority queues
		  • Application QoS in 4-priority queues
		  • Strict priority
		  • VLAN QoS in 4-priority queues
		  • QoS remarking based on IPP/ToS, DSCP and 802.1p
		  • TOS transparency through NAT
		  • Mapping to queue according to DSCP bits and physical port
		  • 802.1Q
		• IGMP proxy v1/v2
		• IGMP snooping v1/v2/v3

Standards	• IEEE 802.11ac • IEEE 802.11n • IEEE 802.11g	• IEEE 802.11b • IEEE 802.3 • IEEE 802.3u
Minimum System Requirements	• Windows 8/7/Vista/XP SP3 or Mac OS X 10.4 or higher • Microsoft Internet Explorer 6 or higher, Firefox 1.0 or higher, Safari 1.2 or higher, or other Java-enabled browser	• Ethernet network interface • Cable or DSL modem • Subscription with an Internet Service Provider (ISP)

WLAN Specifications	• 802.11 n/g/b, up to 150 Mbps • Wi-Fi Protected Setup (WPS) • Multiple SSIDs • Automatic rate adapting • WAN scheduling	• Auto channel selection • WMM support • 64-bit & 128-bit WEP • WPA-PSK & WPA2-PSK • MAC address filtering
Functionality		
Universal Plug and Play Support	• UPnP based auto-configuration • UPnP based port forwarding	• uPnP IGD 1.0

Security	• Attack Prevention
	  • Port scanning & illegal packet attack
	  • DoS Attack
	  • SYN Flooding
	  • Ping of Death
	  • Teardrop
	  • LAND attack
	  • IP Spoofing
	  • IP with zero length
	  • Smurf Attack
	  • TCP Null Scan
		• Stateful Packet Inspection (SPI)
		• Management Access Control for LAN/WAN sides
		• IP filtering
		• MAC filtering
		• URL filter
		• Demilitarized Zone (DMZ)

Device Management	• Web configuration • Telnet management • Webpage/X-Modem/FTP/TFTP firmware upgrade	• Diagnostic tools for ADSL and IP Ping • Setup wizard

Advanced Features	• Multi-language web setup wizard
	• UPnP support
	• DLNA Media Server support
	• VPN pass-through/multi-session PPTP/L2TP/IPSec
		• Dual Active Firewall
		  • Network Address Translation (NAT)
		  • Stateful Packet Inspection (SPI)
		• 802.1p QoS

Physical		
Dimensions	• 213 x 173.2 x 52 mm (8.3 x 6.8 x 2.0 inches)	
Weight	• 401.3 grams (0.88 lbs)	
Temperature	• Operating: 0 to 40 °C (32 to 104 °F)	• Storage: -20 to 65 °C (-4 to 149 °F)
Humidity	• 5 % to 95 % non-condensing	
Certifications	• CE • Wi-Fi	• Wi-Fi Protected Setup (WPS)